ハイエンド・ギガビット・ルーター

SB-7800R ソフトウェアマニュアル
運用ガイド
Ver. 10.7 対応

613-000154 Rev.J 080731

■対象製品

このマニュアルは SB-7800R モデルを対象に記載しています。また，SB-7800R のソフトウェア Ver. 10.7 の機能について記載しています。ソフトウェア機能は，基本ソフトウェア OS-R および各種オプションライセンスによってサポートする機能について記載します。

■日本国外での使用について

弊社製品を日本国外へ持ち出されるお客様は、下記窓口へご相談ください。
　TEL: 0120-860442
　月～金（祝・祭日を除く）9:00 ～ 17:30

■商標一覧

SwitchBlade は，アライドテレシスホールディングス（株）の登録商標です。
Cisco は，米国 Cisco Systems, Inc. の米国および他の国々における登録商標です。
Ethernet は，米国 Xerox Corp. の商品名称です。
GSRP は，アラクサラネットワークス（株）の商標です。
HP OpenView は米国 Hewlett-Packard Company の米国及び他の国々における商品名称です。
Microsoft は，米国およびその他の国における米国 Microsoft Corp. の登録商標です。
NetFlow は米国およびその他の国における米国 Cisco Systems, Inc. の登録商標です。
Octpower は，日本電気（株）の登録商標です。
sFlow は米国およびその他の国における米国 InMon Corp. の登録商標です。
Solaris は，米国及びその他の国における Sun Microsystems, Inc. の商標又は登録商標です。
UNIX は，X/Open Company Limited が独占的にライセンスしている米国ならびに他の国における登録商標です。
Windows は，米国およびその他の国における米国 Microsoft Corp. の登録商標です。
イーサネットは，富士ゼロックス（株）の商品名称です。
そのほかの記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■マニュアルはよく読み，保管してください。

製品を使用する前に，安全上の説明をよく読み，十分理解してください。
このマニュアルは，いつでも参照できるよう，手近な所に保管してください。

■電波障害について

この装置は，情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

■高調波規制について

高調波電流規格　JIS C 61000-3-2 適合品
適合装置：
SB-7804R-AC
SB-7808R-AC
SB-7816R-AC

■ご注意

■マニュアルバージョン

2005 年 5 月 Rev.A 初版
2005 年 7 月 Rev.B
2006 年 1 月 Rev.C
2006 年 4 月 Rev.D
2006 年 6 月 Rev.E
2006 年 8 月 Rev.F
2007 年 6 月 Rev.G
2008 年 3 月 Rev.H
2008 年 7 月 Rev.J

はじめに

■対象製品およびソフトウェアバージョン

このマニュアルは SB-7800R モデルを対象に記載しています。また，SB-7800R のソフトウェア Ver. 10.7 の機能について記載しています。ソフトウェア機能は，基本ソフトウェア OS-R および各種オプションライセンスによってサポートする機能について記載します。
操作を行う前にこのマニュアルをよく読み，書かれている指示や注意を十分に理解してください。また，このマニュアルは必要なときにすぐ参照できるよう使いやすい場所に保管してください。
また，このマニュアルでは特に断らないかぎり基本ソフトウェア OS-R の機能について記載しますが，各種オプションライセンスでサポートする機能を以下のマークで示します。

【OP-BGP】:
　オプションライセンス OP-BGP でサポートする機能です。

【OP-ISIS】:
　オプションライセンス OP-ISIS でサポートする機能です。

【OP-MLT】:
　オプションライセンス OP-MLT でサポートする機能です。

【OP-F64K】:
　オプションライセンス OP-F64K でサポートする機能です。

【OP-ADV】:
　オプションライセンス OP-ADV でサポートする機能です。

【OP-MPLS】:
　オプションライセンス OP-MPLS でサポートする機能です。

■このマニュアルの訂正について

このマニュアルに記載の内容は，ソフトウェアと共に提供する「リリースノート」および「マニュアル訂正資料」で訂正する場合があります。

■対象読者

SB-7800R を利用したネットワークシステムを構築し，運用するシステム管理者の方を対象としています。
また，次に示す知識を理解していることを前提としています。

- ネットワークシステム管理の基礎的な知識

■マニュアルの構成

このマニュアルは，次に示す 10 の章と付録から構成されています。

第 1 章　運用開始前に
　運用管理の概要，および運用開始前に準備するものについて説明しています。

第 2 章　装置起動
　本装置の起動と停止について説明しています。

第 3 章　コマンド操作
　本装置でのコマンドの指定方法について説明しています。

第 4 章　システム操作パネルの操作
本装置でのシステム操作パネルの操作方法について説明しています。

第 5 章　初期導入時の作業
本装置を導入したときに必要な作業について説明しています。

第 6 章　インタフェース状態・ルーティング状態の確認
コンフィグレーションを設定したあとや運用中のトラブル発生時に行う，インタフェース状態およびルーティング状態の確認方法について説明しています。

第 7 章　運用中の作業
本装置がネットワーク上で運用されている間に行う作業について説明しています。

第 8 章　トラブル発生時の対応
本装置が正常に動作しない，通信ができないといったトラブルが発生した場合の対処方法について説明しています。

第 9 章　保守作業
保守関連の作業について説明しています。

第 10 章　ソフトウェアアップデート
ソフトウェアのアップデートやインストールの概念，代表的なトラブルについて説明しています。

付録 A　用語解説
このマニュアルで使用している用語の意味を説明しています。

■このマニュアルの URL

このマニュアルの内容は下記 URL に掲載しておりますので，あわせてご利用ください。
http://www.allied-telesis.co.jp/

■マニュアルの読書手順

本装置の導入，セットアップ，日常運用までの作業フローに従って，それぞれの場合に参照するマニュアルを次に示します。

●ハードウェアの構成，およびソフトウェアの機能を知りたい

解説書 Vol.1
(613-000151)

解説書 Vol.2
(613-000152)

●ハードウェアの設備条件，取扱方法を調べる

SB-7800R
ハードウェア取扱説明書
(613-000150)

●コンフィグレーションの作成方法，設定例

コンフィグレーションガイド
(613-000153)

コンフィグレーション
コマンドレファレンス Vol.1
(613-000155)

コンフィグレーション
コマンドレファレンス Vol.2
(613-000156)

●運用管理方法，トラブルシュート

運用ガイド
(613-000154)

→各コマンドの入力シンタックス，パラメータ詳細

運用コマンドレファレンス
Vol.1
(613-000157)

運用コマンドレファレンス
Vol.2
(613-000158)

→運用ログ詳細

メッセージ・ログレファレンス
(613-000159)

→MIB詳細

MIBレファレンス
(613-000160)

■このマニュアルでの表記

ABR	Available Bit Rate
AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
ATM	Asynchronous Transfer Mode

AUX	Auxiliary
BCU	Basic management Control module
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second　　*bpsと表記する場合もあります。
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CBR	Constant Bit Rate
CDP	Cisco Discovery Protocol
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CP	multi layer Control Processor
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
Diff-serv	Differentiated Services
DIS	Draft International Standard/Designated Intermediate System
DLCI	Data Link Connection Identifier
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EFM	Ethernet in the First Mile
ES	End System
FCS	Frame Check Sequence
FDB	Filtering DataBase
FR	Frame Relay
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GFR	Guaranteed Frame Rate
HDLC	High level Data Link Control
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IIH	IS-IS Hello
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
IS	Intermediate System
IS-IS	Information technology - Telecommunications and Information exchange between systems - Intermediate system to Intermediate system Intra-Domain routeing information exchange protocol for use in conjunction with the Protocol for providing the Connectionless-mode Network Service (ISO 8473)
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path

LSP	Link State PDU
LSR	Label Switched Router
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MIB	Management Information Base
MPLS	Multi-Protocol Label Switching
MRU	Maximum Receive Unit
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NIF	Network Interface board
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations, Administration, and Maintenance
OSI	Open Systems Interconnection
OSINLCP	OSI Network Layer Control Protocol
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
PAD	PADding
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
POH	Path Over Head
POS	PPP over SONET/SDH
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PRI	Primary Rate Interface
PRU	Packet Routing Module
PSNP	Partial Sequence Numbers PDU
PVC	Permanent Virtual Channel (Connection)/Permanent Virtual Circuit
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RM	Routing Manager
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
SA	Source Address
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SOH	Section Over Head
SONET	Synchronous Optical Network
SOP	System Operational Panel
SPF	Shortest Path First
SSAP	Source Service Access Point

```
TA          Terminal Adapter
TACACS+     Terminal Access Controller Access Control System Plus
TCP/IP      Transmission Control Protocol/Internet Protocol
TLA ID      Top-Level Aggregation Identifier
TLV         Type, Length, and Value
TOS         Type Of Service
TPID        Tag Protocol Identifier
TTL         Time To Live
UBR         Unspecified Bit Rate
UDLD        Uni-Directional Link Detection
UDP         User Datagram Protocol
UPC         Usage Parameter Control
UPC-RED     Usage Parameter Control - Random Early Detection
VBR         Variable Bit Rate
VC          Virtual Channel/Virtual Call/Virtual Circuit
VCI         Virtual Channel Identifier
VLAN        Virtual LAN
VP          Virtual Path
VPI         Virtual Path Identifier
VPN         Virtual Private Network
VRRP        Virtual Router Redundancy Protocol
WAN         Wide Area Network
WDM         Wavelength Division Multiplexing
WFQ         Weighted Fair Queueing
WRED        Weighted Random Early Detection
WS          Work Station
WWW         World-Wide Web
XFP         10 gigabit small Form factor Pluggable
```

■常用漢字以外の漢字の使用について

このマニュアルでは，常用漢字を使用することを基本としていますが，次に示す用語については，常用漢字以外を使用しています。

- 宛て（あて）
- 宛先（あてさき）
- 迂回（うかい）
- 鍵（かぎ）
- 個所（かしょ）
- 筐体（きょうたい）
- 桁（けた）
- 毎（ごと）
- 閾値（しきいち）
- 芯（しん）
- 溜まる（たまる）
- 必須（ひっす）
- 輻輳（ふくそう）
- 閉塞（へいそく）
- 漏洩（ろうえい）

■ kB(バイト) などの単位表記について

1kB(キロバイト)，1MB(メガバイト)，1GB(ギガバイト)，1TB(テラバイト) はそれぞれ 1,024 バイト，1,024 ^{2} バイト，1,024 ^{3} バイト，1,024 ^{4} バイトです。

目次

5 初期導入時の作業

6 インタフェース状態・ルーティング状態の確認

1 運用開始前に

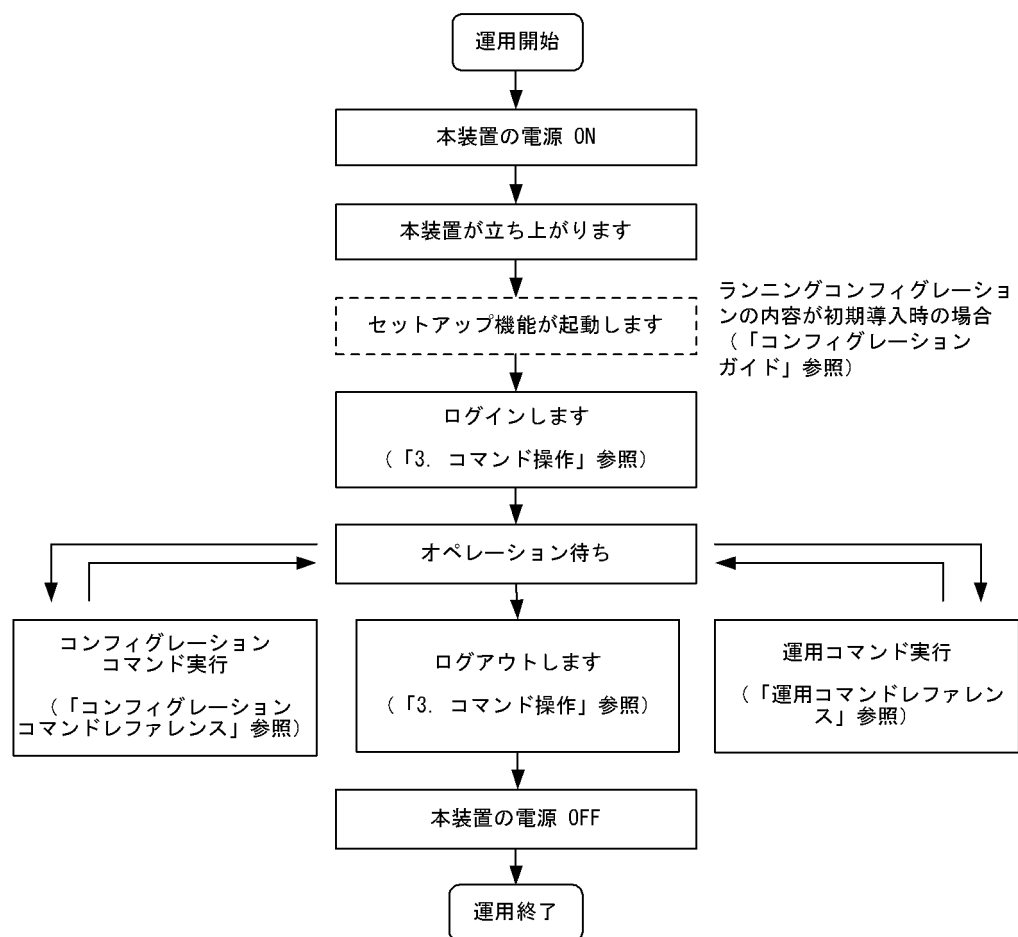
この章では，運用管理の概要，および運用を開始する前に準備するものについて説明します。

1.1　運用管理の概要

本装置はセットアップ作業が終了し，装置の電源 ON で運用に入ります。本装置と接続した運用端末では，運用コマンドやコンフィグレーションコマンドを実行し，装置の状態を調べたり，接続ネットワークの変更に伴うコンフィグレーションの変更を実施したりできます。運用端末の種類を「表 1-1　運用端末の種類」に，運用管理の概略を「図 1-1　運用管理の概略」に示します。

表 1-1　運用端末の種類

項番	種類	概要
1	コンソール	本装置と RS232C ケーブルで接続する端末
2	リモート運用端末（リモートログイン）	本装置と TCP ／ IP で通信できる端末で，telnet などでリモートログインする端末

図 1-1　運用管理の概略

1.2　本装置を運用する上での準備品

1.2.1　コンソール

本装置の初期導入時に運用端末として必要になるのがコンソールです。コンソールはRS-232Cに接続する端末で，一般的な通信端末，通信ソフトウェアが使用可能です。

（1）通信ソフトウェア

以下の通信ソフトまたはそれに準ずる通信ソフトを使用してください。

● Microsoft Windows 2000／Windows XP付属のハイパーターミナル

（2）通信ソフトウェアの設定値確認

コンソールが本装置と通信できるように，次の標準VT-100設定値（本装置のデフォルト設定値）が通信ソフトウェアに設定されていることを確認してください。

● 通信速度：9600bps

● データ長：8ビット

● パリティビット：なし

● ストップビット：1ビット

● フロー制御：なし

なお，通信速度に9600bps以外（1200／2400／4800／19200bps）を設定して使用したい場合は，コンフィグレーションコマンドsystemで本装置側の通信速度設定を変更してください。ただし，実際に設定が反映されるのはコンソールからいったんログアウトしたあとです。

（3）通信ソフトウェア使用上の注意

「(1) 通信ソフトウェア」で挙げた通信ソフトウェアには，次に示す注意事項があります。

（a）ハイパーターミナル

接続中に通信速度を変更しても実際の通信速度は変更されません。ただし，ステータスバーの表示は変更後の値になります。ツールバーから切断，接続を行って通信速度を変更してください。

（4）RS-232C

RMシリアル接続（RS232C）の本装置のシリアルインタフェースはD-Sub9ピンです。コンソールと接続する場合にはクロスケーブルを使用してください。例えば，AT互換機と本装置を接続する場合には，AT互換機同士をシリアルで接続するためのD-Sub9ピンクロスケーブルを使用してください。クロスケーブルの結線仕様を次の図に示します。

図 1-2 クロスケーブルの結線仕様

項番	本装置側 9 ピン（メス）		接　続	セットアップ端末側 9 ピン（メス）	
	ピン番号	信号名		ピン番号	信号名
1	5	SG		5	GND
2	3	SD		2	RX
3	2	RD		3	TX
4	7	RS		1	DCD
5	8	CS		8	CTS
6	1	CD		7	RTS
7	6	DR		4	DTR
8	4	ER		6	DSR

(5) モデム

AUX を使ってダイアルアップ IP 接続を行う場合（操作方法は「5.9 ダイアルアップ IP 接続を設定する」を参照），または RM シリアル接続を行う場合，モデムやモデムと AT 互換機を接続するためのストレートケーブルを用意してください。また，本装置に接続するモデムは自動着信に設定してください。本装置ではモデムを設定できないので，PC などに接続して設定してください。

また，モデムに付属の説明書を参照し，AT コマンドを使用して次の表に示す設定を行ってください。拡張 AT コマンドを持つモデムでは，例で示したコマンドと異なるコマンドを使用する場合があります。

表 1-2 モデムの設定

設定項目	設定内容	指定例（Hayes 互換 AT コマンドの場合）
CD 信号状態	CD 信号は通常オフで，相手モデムのキャリアを受信するとオンにします。	AT&C1
DTR 信号状態	DTR 信号がオンからオフに変わるとモデムを初期化します。	AT&D3
コマンドエコー	入力したコマンドを DTE に出力しません。	ATE0
フロー制御	DTE と DCE 間のフロー制御を設定します。 • RTS/CTS フロー制御有効 • XON/XOFF フロー制御無効	AT&K3
リザルトコード	リザルトコードを DTE に出力しません。	ATQ1
自動着信	自動着信するまでの呼び出し回数を設定します。	ATS0=2
リセット時の設定	モデム内の不揮発性メモリから設定を読み出します。	AT&Y0
設定の保存	設定をモデム内の不揮発性メモリに保存します。	AT&W0

コマンドを DTE に出力しないようにコマンドエコーを設定すると，コマンドを入力しても文字は表示されません。設定が完了したらモデムに設定内容を保存します。設定保存後に設定内容を表示して確認します。

（例）Hayes 互換 AT コマンドでモデムを自動着信に設定する場合
　AT&F&C1&D3E0&K3Q1S0=2&W0&Y0&V

RM シリアル接続（モデム）の場合は，通信ソフトウェアのダイアル機能を使用してダイアルします。ダイアルの設定は通信ソフトウェアの説明を参照してください。端末から AT コマンドを使用してダイアル接続できます。ダイアル機能を持たない通信ソフトウェアを使用する場合などは AT コマンドでダイアルしてください。AT コマンドのダイアル方法についてはモデムのマニュアルを参照してください。

（例）Hayes 互換 AT コマンドでダイアルする場合

- 公衆回線を使用してトーンで 123-4567 へダイアルする
  AT&FE0&S1S0=0S2=255TD123-4567
- 構内交換機を使用してトーンで 123-4567 へダイアルする
  AT&FX3E0&S1S0=0S2=255TD123-4567
- 構内交換機を使用してトーンで 0 をダイアルして，数秒待ってから 123-4567 へダイアルする
  AT&FX3E0&S1S0=0S2=255TD0,123-4567

1.2.2 リモート運用端末

本装置に，IP ネットワーク経由で接続してコマンド操作を行う端末が，リモート運用端末です。telnet，rlogin，および ftp プロトコルのクライアント機能がある端末はすべてリモート運用端末として使用できます。

(a) Windows Telnet をリモート運用端末として使用する場合

Windows Telnet を使用して本装置に Telnet ログインする場合，Windows Telnet 改行コードの設定を画面上で変更する必要があります。次に示す手順で設定をしてください。一度設定すれば Windows 端末の電源を OFF/ON しても設定内容は保存されます。

1. コマンドプロンプトから Windows 付属の Telnet をオプションなしで起動します。
   ```
   C:¥Windows>telnet
   ```
2. Windows Telnet の画面がプロンプト付きで表示されるので，unset CRLF を実行します。
   ```
   Microsoft Telnet> unset CRLF
   ```

1.2.3 バックアップ用 MC

MC には，本装置の制御プログラムやコンフィグレーションなどが格納されます。そのため，MC が故障すると本装置の立ち上げができなくなります。MC 故障時に迅速な復旧（故障 MC の交換）をするため，ご発注時に MC を 2 枚購入されていない場合は，別途バックアップ用 MC として MC をもう 1 枚追加購入されることをお勧めします。

また，MC が 2 枚あれば次の表に示す運用も可能です。

表 1-3 2 枚の MC による運用方法

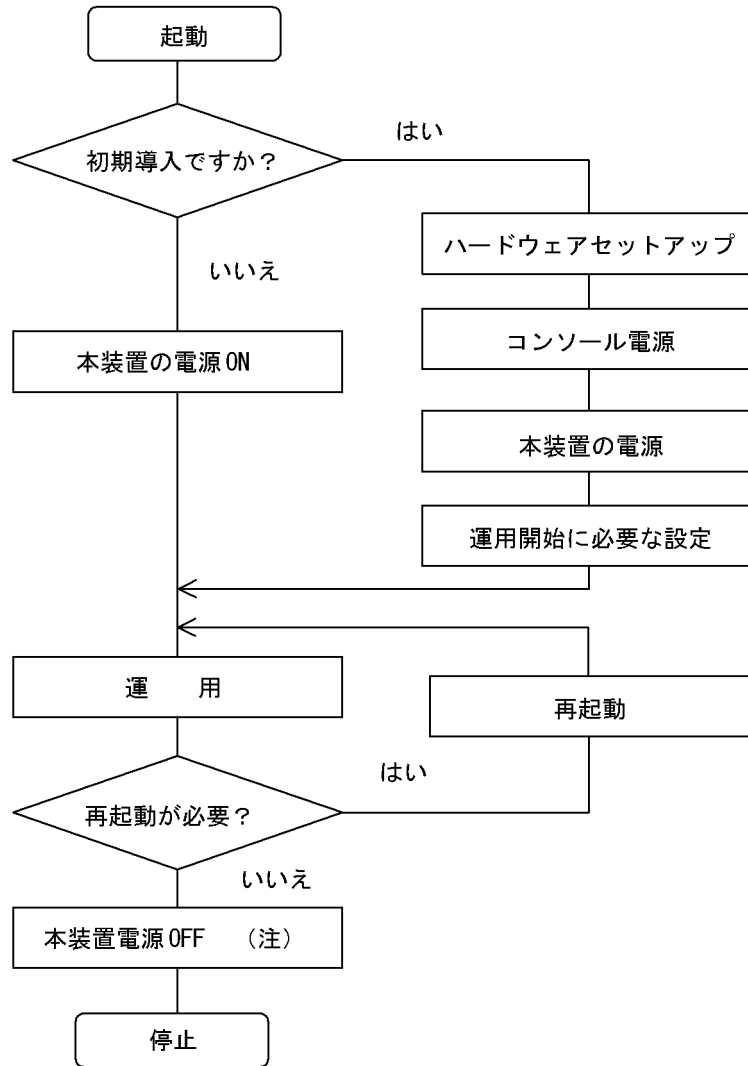
運用方法	詳細
予備 MC によるバックアップ運用	予備の MC は，MC または MC スロットの障害時のバックアップとして使用します。この場合，コンフィグレーションの変更は常に反映して同一内容にする必要があります。
コンフィグレーションの 2 世代管理運用	2 種類のコンフィグレーションを切り替えて使用します。スロット 0 とスロット 1 の MC に異なるコンフィグレーションを入れておき，優先 MC スロットの設定を変更して起動することでコンフィグレーションを切り替えます。この場合，MC はバックアップとして使用できません。
ソフトウェアバージョンの 2 世代管理運用	2 種類のソフトウェアバージョンを切り替えて使用します。スロット 0 とスロット 1 の MC に異なるソフトウェアバージョンを入れておき，優先 MC スロットの設定を変更して起動することで，ソフトウェアバージョンを切り替えます。この場合，MC はバックアップとして使用できません。

2 装置起動

この章では，装置の起動と停止について説明します。

2.1　起動から停止までの概略

本装置の起動から停止までの概略フローを次の図に示します。ハードウェアセットアップの内容については「ハードウェア取扱説明書」を参照してください。

図 2-1　起動から停止までの概略フロー

注　MC にアクセスしているときに電源 OFF すると，MC を破損する場合があります。

2.2 装置を起動する

本装置の起動，再起動の方法を，次の表に示します。

表 2-1 起動，再起動の方法

項番	起動の種類	内容	操作方法
1	電源 ON による起動	本装置の電源 OFF からの立ち上げです。	本体の電源スイッチを ON にします。
2	リセットによる再起動	障害発生などにより，本装置をリセットしたい場合に行います。	本体のリセットスイッチを押します。
3	コマンドによる再起動	障害発生などにより，本装置をリセットしたい場合に行います。	reload コマンドを実行します。
4	デフォルトリスタート	パスワードを忘れた場合に行います。パスワードによるセキュリティチェックを行わないのでデフォルトリスタートによる起動を行う場合は十分に注意してください。なお，アカウント，コンフィグレーションはデフォルトリスタート前のものが使用されます。	システム操作パネルの FWRD キーと BACK キーを押しながら，リセットスイッチを押します。

本装置を起動，再起動したときに STATUS ランプが赤点灯となった場合は，「8.1.2 STATUS ランプが緑点灯以外の状態である」を参照してください。また LED ランプ表示内容の詳細は，「ハードウェア取扱説明書」を参照してください。

2.3 装置を停止する

- 本装置の電源を OFF する場合は，MC にアクセスしていないことを確認して行ってください。MC のスロットごとに MC アクセスを示す LED があります。電源を OFF するときは，LED が消灯している（MC にアクセスしていない）ことを確認してください。LED が点灯している（MC にアクセスしている）ときに電源を OFF すると，MC を破損する場合があります。
  また，ログの自動保存によって MC にアクセスする場合がありますので，電源を OFF する際にはご注意ください。ログを自動保存する契機については，「メッセージ・ログレファレンス　1.4.6 ログの自動保存と参照」を参照してください。
- 運用コマンドまたはコンフィグレーションコマンドを実行したあと，すぐに電源を OFF する必要がある場合は，システム操作パネルから shutdown 指示したあと電源を OFF するか，reload stop コマンドで装置を停止させたあとに電源を OFF してください。

2.4　コンソールからログインする

装置起動後，コンソールには次の図に示すメッセージが表示されます。最後にログインプロンプトが表示されるので，そこで本装置にログインしてください。ログインの実行例については，「3.1　CLI での操作（1）ログイン」を参照してください。

図 2-2　装置起動時のメッセージ

```
08/18 11:17:30 Starting 1st loader

ROM 03-02 Rev6 Wed Mar  6 13:05:59 2002 JST
BIOS Rev.:R1.02.E4 (990129)

08/18 11:17:33 Loading from MC slot 0

08/18 11:17:33 Starting 2nd loader
08/18 11:17:33 Loading /boot ... done.


08/18 11:17:34 Starting 3rd loader
08/18 11:17:35 Loading /bsd.0000.gz ... done.
08/18 11:17:37 Loading rdimage.gz ... done.(08/18 11:17:42 )
08/18 11:17:42 Loading rdimage2.gz ... done.(08/18 11:17:43 )

login:
```

2.4.1　初期導入時のログイン

初期導入時にログインする場合，次のアカウント名を使用してください。

アカウント名：operator

パスワード：なし

3 コマンド操作

この章では，本装置でのコマンドの指定方法について説明します。

3.1 CLI での操作

3.1.1 ログイン・ログアウト

(1) ログイン

ログイン画面を次の図に示します。この画面でユーザ名とパスワードを入力してください。正しく認証された場合は，CLI プロンプトが表示されます。また，認証に失敗した場合は”Login incorrect”のメッセージが表示されます。

図 3-1 ログイン画面

(2) ログアウト

CLI での操作を終了してログアウトしたい場合には logout コマンドまたは exit コマンドを実行してください。次の図に実行画面を示します。

図 3-2 ログアウト

```
> logout
login:
```

3.1.2 コマンド入力モード

本装置でコンフィグレーションの変更を実施したり，または装置の状態を参照したりする場合，適切なコマンド入力モードに遷移し，コンフィグレーションコマンドや運用コマンドを入力する必要があります。

コマンド入力モードとモード移行コマンドの関係を次の図に示します。

図 3-3　コマンド入力モードとモード移行コマンド

表 3-1　コマンド入力モードとプロンプトの対応

コマンド入力モード	実行可能なコマンド	プロンプト
一般ユーザモード	運用コマンド（configure，adduser コマンドなど，一部のコマンドは装置管理者モードで実行可能です。）	>
装置管理者モード	運用コマンド	#
コンフィグレーションモード※	コンフィグレーションコマンド	(config)#

注※

コンフィグレーションモードで運用コマンドを実行したい場合，quit コマンドや exit コマンドによってコマンド入力モードを装置管理者モードに切り替えなくても，運用コマンドの先頭に「$」を付けた形式で入力することで実行できます。

＜例＞

コンフィグレーションモードで show ip arp コマンドを実行する場合

```
(config)# $show ip arp
```

また，CLI プロンプトとして，次に示す場合でも，その状態を意味する文字がプロンプトの先頭に表示されます。

1. コンフィグレーションコマンド system の name パラメータで本装置のホスト名称を設定している場合，プロンプトに反映されます。
2. ランニングコンフィグレーションを編集し，その内容をスタートアップコンフィグレーションに保存していない場合，プロンプトの先頭に”！”が付きます。
3. IPv4 ルーティングプロトコル情報，IPv6 ルーティングプロトコル情報および MPLS 情報を編集し，コンフィグレーションコマンド apply でその内容をランニングコンフィグレーションに反映していない場合は，プロンプトの先頭に”!!”が付きます。

1. ～ 3. の表示例を次の図に示します。

図 3-4　プロンプト表示例

```
> enable
# configure
(config)# system name "System name"
!System name(config)# save
System name(config)# static 192.168.201.0 masklen 24 gateway 172.16.178.2
!!System name(config)# apply
!System name(config)# save
System name(config)# quit
System name# quit
System name>
```

3.1.3　CLI 機能

(1) 補完機能

コマンドライン上で［Tab］を入力することで，コマンド入力時のコマンド名称やファイル名の入力を少なくでき，コマンド入力が簡単になります。次の図に補完機能を使用したコマンド入力の簡略化を示します。

図 3-5　補完機能を使用したコマンド入力の簡略化

```
(config)# li[Tab]
line        link-aggregation
(config)# lin
```

［Tab］押下で使用できるパラメータやファイル名の一覧が表示されます。

```
(config)# line line0 [Tab]
10gigabit_ethernet ethernet gigabit_ethernet
(config)# line line0 [Tab]
```

(2) ヘルプ機能

コマンドライン上で［?］を入力することで，指定できるコマンドまたはパラメータを検索できます。また，コマンドやパラメータの意味を知ることができます。次の図に［?］入力時の表示例を示します。

図 3-6　［?］入力時の表示例

```
> show ip ?
  arp         Display the information of ARP
  cache       Display the conditions of policy route group information
  entry       Display a detail information of a particular route
  interface   Display the information of interface
  local       Display summarized policy routing information
  policy      Display Policy Routing Information
  rip         Display RIP information
  route       Display all route
  static      Display the information of STATIC
>
```

なお，パラメータの入力途中でスペース文字を入れずに［?］を入力した場合は，補完機能が実行されます。

また，コマンドパラメータで ? 文字を使用する場合は，［Ctrl］＋［V］を入力後，［?］を入力してください。

(3) 入力エラー位置指摘機能

コマンドまたはパラメータを不正に入力した際，エラー位置を”＾”で指摘し，次行にエラーメッセージ（「運用コマンドレファレンス Vol.1　入力エラー位置指摘で表示するメッセージ」を参照）を表示します。［Tab］入力時と［?］入力時も同様となります。

”＾”の指摘個所とエラーメッセージの説明により，コマンドまたはパラメータを修正し再度入力してください。入力エラー位置指摘の表示例を「図 3-7　スペルミス時の表示例」～「図 3-9　パラメータ入力途中の表示例」に示します。

図 3-7　スペルミス時の表示例

```
(config)# line line0 ehternet 1/0
line line0 ehternet 1/0
            ^
% illegal parameter at '^' marker
(config)#
```

図 3-8　同じパラメータを 2 回入力したときの表示例

```
(config)# line line0 ethernet 0/0
[line line0]
(config)# type 10m_full_duplex type auto_negotiation
type 10m_full_duplex type auto_negotiation
                      ^
% illegal combination or already appeared at '^' marker
[line line0]
(config)#
```

図 3-9　パラメータ入力途中の表示例

```
(config)# line line0 ethernet 0/0
[line line0]
(config)# type
type
      ^
% Incomplete command at '^' marker
[line line0]
(config)#
```

(4) コマンド短縮実行

コマンドまたはパラメータを短縮して入力し，入力された文字が一意のコマンドまたはパラメータとして認識できる場合，コマンドを実行します。次の図に短縮入力のコマンド実行例を示します。

図 3-10　短縮入力のコマンド実行例（show ip interface の短縮入力）

```
> sh ip in[Enter]
Tokyo: flags=80e2<DOWN,BROADCAST,NOTRAILERS,RUNNING,NOARP,MULTICAST>
        mtu 1536
        inet 10.1.1.1/24 broadcast 10.1.1.255
        NIF0/Line0: DOWN media - 00:12:E2:98:dc:50
        Time-since-last-status-change: 00:00:54
        Last down at: -----
>
```

なお，「コンフィグレーションコマンドレファレンス Vol.1　2. コンフィグレーション操作コマンド」にあるコマンドは，コンフィグレーションモードの第一階層以外で短縮実行できません。

(5) ヒストリ機能

ヒストリ機能を使用すると，過去に入力したコマンドを簡単な操作で再実行したり，過去に入力したコマンドの一部を変更して再実行したりできます。次の図にヒストリ機能を使用した例を示します。

図 3-11 ヒストリ機能を使用したコマンド入力の簡略化

```
> ping 192.168.0.1 numeric count 1              ←―――― 192.168.0.1に対してpingコマンドを実行
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=31 time=1.329 ms

--- 192.168.0.1 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.329/1.329/1.329 ms
>________
 |
 |       ↑キーを入力することにより前に入力したコマンドを呼び出すことができます
 |       この例の場合↑キーを１回押すと"ping 192.168.0.1 numeric count 1"が表示されるので,
 |       リターンキーの入力だけで同じコマンドを再度実行することができます
 ↓
> ping 192.168.0.1 numeric count 1              ←―――― 192.168.0.1に対してpingコマンドを実行
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=31 time=1.225 ms

--- 192.168.0.1 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.225/1.225/1.225 ms
>________
 |
 |       ↑キーを入力することにより前に入力したコマンドを呼び出し，←キー，Deleteキーを
 |       使ってコマンド文字列を編集することができます
 |       この例の場合↑キーを１回押すと"ping 192.168.0.1 numeric count 1"が表示されるので,
 |       IPアドレスの"1"の部分を"2"に変更しリターンキーを入力しています
 ↓
> ping 192.168.0.2 numeric count 1              ←―――― 192.168.0.2に対してpingコマンドを実行
PING 192.168.0.2 (192.168.0.2): 56 data bytes

--- 192.168.0.2 ping statistics ---
1 packets transmitted, 0 packets received, 100% packet loss
>
```

ヒストリ機能に次の表に示す文字列を使用した場合には，コマンド実行前に過去に実行したコマンド文字列に変換したあとにコマンドを実行します。なお，コンフィグレーションコマンドではコマンド文字列変換はサポートしていません。

表 3-2 ヒストリのコマンド文字列変換で使用できる文字一覧

項番	指定	説明
1	!!	直前に実行したコマンドへ変換して実行します。
2	!n	ヒストリ番号 n※のコマンドへ変換して実行します。
3	!-n	n 回前のコマンドへ変換して実行します。
4	!str	文字列 str で始まる過去に実行した最新のコマンドへ変換して実行します。
5	^str1^str2	直前に実行したコマンドの文字列 str1 を str2 に置換して実行します。

注※ show history コマンドで表示される配列番号のこと

注意事項

通信ソフトウェアによって方向キー（[↑]，[↓]，[←]，[→]）を入力してもコマンドが呼び出されない場合があります。その場合は通信ソフトウェアのマニュアルなどにより設定を確認してください。

(6) パイプ機能

パイプ機能を利用することにより，コマンドの実行結果を別のコマンドに引き継げます。実行結果を引き継ぐコマンドに grep コマンドや sort コマンドを使うことにより，コマンドの実行結果をよりわかりやす

くすることができます。「図 3-12　show sessions コマンド実行結果」に show sessions コマンドの実行結果を，「図 3-13　show sessions コマンド実行結果を grep コマンドでフィルタリング」に show sessions コマンドの実行結果を grep コマンドでフィルタリングした結果を示します。また，「図 3-14　show ip interface コマンド実行結果」に show ip interface コマンドの実行結果を，「図 3-15　show ip interface コマンド実行結果を sort コマンドでフィルタリング」に show ip interface コマンドの実行結果を sort コマンドでフィルタリングした結果を示します。

図 3-12　show sessions コマンド実行結果

```
> show sessions
operator         console  -----  0  Jul  7 10:57:30
operator         ttyp0    -----  1  Jul  7 10:13:01 (192.168.3.7)
operator         ttyp1    -----  2  Jul  7 10:49:49 (192.168.3.7)
operator         ttyp2    admin  3  Jul  7 11:06:41 (192.168.3.7)
>
```

図 3-13　show sessions コマンド実行結果を grep コマンドでフィルタリング

```
> show sessions | grep admin
operator         ttyp2    admin  3  Jul  7 11:06:41 (192.168.3.7)
>
```

図 3-14　show ip interface コマンド実行結果

```
> show ip interface summary
tokyo: UP  192.168.0.1  255.255.255.0
nagoya: UP  192.168.1.1  255.255.255.0
osaka: DOWN  192.168.2.1  255.255.255.0
fukuoka: UP  192.168.3.1  255.255.255.0
sapporo: DOWN  192.168.4.1  255.255.255.0
>
```

図 3-15　show ip interface コマンド実行結果を sort コマンドでフィルタリング

```
> show ip interface summary | sort
fukuoka: UP  192.168.3.1  255.255.255.0
nagoya: UP  192.168.1.1  255.255.255.0
osaka: DOWN  192.168.2.1  255.255.255.0
sapporo: DOWN  192.168.4.1  255.255.255.0
tokyo: UP  192.168.0.1  255.255.255.0
>
```

(7) リダイレクト

リダイレクト機能を利用することにより，コマンドの実行結果をファイルに格納できます。次の図に show interfaces コマンドの実行結果をファイルに格納する例を示します。

図 3-16　show interfaces コマンド実行結果をファイルに出力

```
> show interfaces nif 0 line 0 > show_interface.log
>
```

(8) ページング

コマンドの実行により出力される表示について，表示すべき情報が一画面にすべて表示しきれない場合には，ユーザのキー入力を契機に一画面ごとに区切って表示します。ただし，リダイレクトのあるときにはページングを行いません。なお，ページングはコンフィグレーションコマンド login または運用コマンド set terminal pager でその機能を有効にしたり無効にしたりできます。

(9) 警告メッセージ

装置の状態を変更して，その状態のままにしておくと運用に支障がある場合があります。例えば，回線テストコマンドを実行すると該当回線は回線テスト状態のままになり，運用状態にはならないため該当回線を使用した通信が行えません。このように運用に支障がある状態にした場合には，警告メッセージがある旨のメッセージ「You have warning messages. Use ” show warning” to see them.」を表示するので，show warning コマンドを用いて警告メッセージを確認してください。また，コンフィグレーションマンド login または運用コマンド set terminal warning-level によりその表示レベルを変更できます。警告メッセージの内容を次の表に示します。

表 3-3 警告メッセージ一覧

メッセージ	内容
mc0 is disable	MC0 が使用禁止状態になっています。MC へのアクセスができないため，正常なオペレーションができない可能性があります。
mc1 is disable	MC1 が使用禁止状態になっています。MC へのアクセスができないため，正常なオペレーションができない可能性があります。
This System is restarted by pressing default-restart-switch	デフォルトリスタートによって装置が起動されています。パスワードによるセキュリティチェックが動作していないので注意してください。
Version mismatch between active and standby software detected.	運用系と待機系でソフトウェアのバージョンが異なっています。
Date mismatch between active and standby configuration files detected.	運用系と待機系でコンフィグレーションが異なっています。
NIF <NIF No.> Line <Line No.> is under line-test	該当回線が回線テスト中になっています。該当回線は運用していません。 <NIF No.> : NIF 番号 <Line No.> : Line 番号 <Subline No.> : Subline 番号
NIF <NIF No.> Line <Line No.> subline <Subline No.> is under line-test	
Half a year has passed since first dump file creation. ※	運用系の”/dump0”,”/dump1”,”/primaryMC/usr/var/evtdump”配下に，作成から半年以上経過しているダンプファイルが一つ以上あります。ダンプファイルの整理をしてください。不要なダンプファイルを削除する際は，erase dumpfile コマンド（「運用コマンドレファレンス Vol.1 erase dumpfile」）を参照してください。

注※ 装置の現在時刻とダンプファイルの作成時刻を比較しているため，ダンプファイル作成後に set calendar コマンド（「運用コマンドレファレンス Vol.1 set calendar」参照）で装置の時間を変更した場合，本警告メッセージが表示されることがあります。

(10) 運用メッセージ

装置の状態が変化した場合は運用メッセージをコンソールやリモート運用端末に表示します。例えば，回線が障害状態から回復した場合は回線が回復したメッセージを，回線が障害になり運用を停止した場合は回線が障害になったメッセージを表示します。運用メッセージの詳細については，「メッセージ・ログレファレンス 2. ルーティングプロトコルのイベント情報」を参照してください。なお，シェルプログラム実行時や高負荷時には運用メッセージが表示されない場合がありますが，ログ情報にすべての運用メッセージが記録されているので，ログ情報で確認してください。

(11) 自動ログアウト

一定時間（デフォルト：60 分）内にキー入力がなかった場合には自動的にログアウトします。なお，自動ログアウト時間はコンフィグレーションコマンド login または運用コマンド set exec-timeout で変更できます。

3.1.4 CLI 設定のカスタマイズ

CLI 機能の一部は，ユーザごとに CLI 環境情報を設定することで，動作をカスタマイズできます。カスタマイズ可能な CLI 機能と CLI 環境情報を次の表に示します。

表 3-4 カスタマイズ可能な CLI 機能と CLI 環境情報

項番	機能	カスタマイズ内容と初期導入時のデフォルト設定
1	自動ログアウト	自動ログアウトするまでの時間を設定できます。 初期導入時のデフォルト設定は，60 分です。
2	ページング	ページングするかどうかを設定できます。 初期導入時のデフォルト設定は，ページングをします。
3	ヘルプ機能	ヘルプメッセージで表示するコマンドの一覧を設定できます。 初期導入時のデフォルト設定は，運用コマンドのヘルプメッセージを表示する際に，入力可能なすべての運用コマンドの一覧を表示します。
4	警告がある旨のメッセージ	「警告がある旨のメッセージ」の出力レベルを設定できます。 初期導入時のデフォルト設定は，警告があるときに，常に「警告がある旨のメッセージ」を表示します。ただし，運用コマンド adduser で no-mc パラメータを指定して追加したアカウントのデフォルト設定は，警告があるときでも，「警告がある旨のメッセージ」を表示しません。
5	コマンド入力モード	CLI 運用コマンドのコマンド入力モードを変更します。 初期導入時のデフォルト設定は，新シンタックス運用コマンドモードです。

これらの CLI 環境情報は，ユーザごとに，コンフィグレーションコマンド login または次に示す運用コマンドで設定できます。

- set exec-timeout
- set terminal pager
- set terminal help
- set terminal warning-level
- set terminal command-literal

コンフィグレーションコマンド login による設定は，運用コマンドによる設定よりも優先されます。五つの CLI 環境情報のうち，どれか一つでもコンフィグレーションコマンドで設定した場合，その対象ユーザは，運用コマンドによる設定値は使用されません。コンフィグレーションコマンドの設定値または省略時の初期値で動作します。

なお，コンフィグレーションコマンドによる設定内容は，次回のログインから動作に反映されます。

運用コマンドによる設定は，コンフィグレーションコマンドによる設定がない場合に使用されます。コンフィグレーションコマンドで一つも CLI 環境情報を設定していないユーザは，運用コマンドによる設定値が使用されます。なお，運用コマンドによる設定では，設定状態を表示できないため，各機能の動作状態で確認してください。

運用コマンドによる設定内容は，コマンド実行直後から動作に反映されます。さらに，コンフィグレーションコマンドによる設定で動作している場合でも，一時的に該当セッションでの動作を変更できます。

なお，運用コマンドによる設定の場合，adduser コマンドで no-mc パラメータを指定して追加したアカウントのユーザは，装置を再起動したときに，CLI 環境情報が初期導入時のデフォルト設定に戻ります。

運用コマンドで設定した CLI 環境情報を待機系システムに同期させるには，synchronize コマンドで userfile パラメータまたは account パラメータを指定して実行してください。

3.2　CLI の注意事項

3.2.1　自動ログアウト時の注意

コンフィグレーションを編集中のまま自動ログアウトした場合は，コンフィグレーションの編集中のままの状態になります。

3.2.2　ログイン後に運用端末がダウンした場合

ログイン後，運用端末がダウンした場合，本装置内ではログインしたままの状態になっていることがあります。この場合，自動ログアウトを待つか，再度ログインし直してログインしたままの状態になっているユーザを killuser コマンドで削除してください。また，コンフィグレーション編集中の場合は，「3.2.1 自動ログアウト時の注意」と同じようにコンフィグレーションの編集中になっているので，configure コマンド実行後，コンフィグレーションコマンド quit(exit) でコンフィグレーションの編集を終了させてください。

3.2.3　待機系の MC にあるファイルにアクセスする場合

待機系のファイルを /standby ディレクトリで参照する場合，次の制限があります。

1. 補完機能は使用できません。
2. /standby は，配下のディレクトリに cd（チェンジディレクトリ）しないでください。
3. /standby は，配下のファイルアクセスは運用系のファイルアクセスに比べて時間がかかります。

3.2.4　待機系でコマンドを実行した場合

待機系では一部のコマンドは実行できません。コマンドは運用系で実行するようにしてください。なお，待機系にログインしているかどうかは，次の図のようにプロンプト表示（”SBY:”が付く）で判別できます。

図 3-17　待機系にログインした場合のプロンプト表示

```
login: user1
Password: *******
Copyright (c) 2005 Allied Telesis Holdings K.K. All rights reserved.
*** Welcome to the System ***
SBY:>
```

3.2.5　telnet 接続時の注意事項

telnet 接続で本装置にログインしている場合，コマンド実行中は telnet セッションを切断しないでください。

コマンド実行中に telnet セッションが切断された場合は，実行中のコマンドが途中終了している可能性があるので，本装置に再度ログイン後，コマンドを再実行してください。

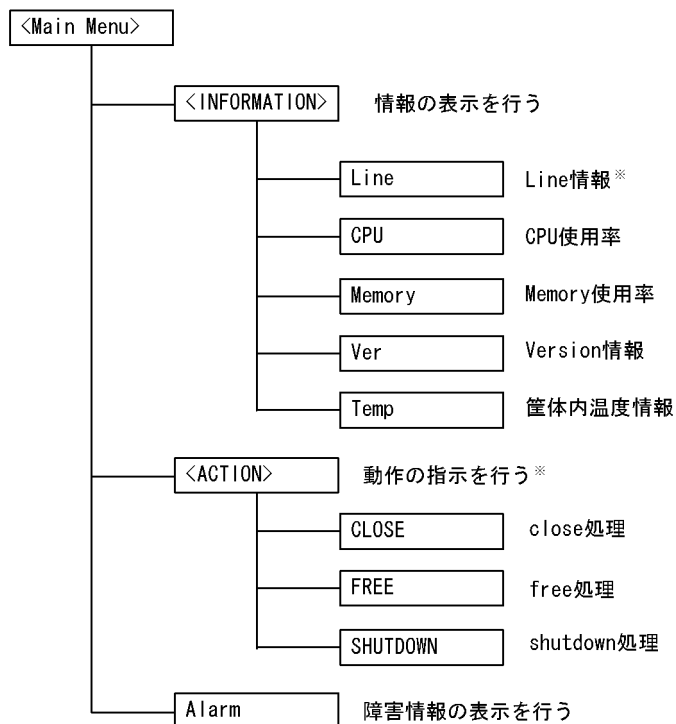
それでも異常が解消されない場合は，保守員に連絡してください。

4 システム操作パネルの操作

この章では，システム操作パネルの操作方法について説明しています。
システム操作パネルは BACK キー（◀），ENTR キー（■），FWRD キー（▶）の三つの操作キーを持ち，これらの操作キーを操作することで，装置情報の表示や動作指示，障害情報の表示を行うことができます。
メニューでは，操作キーの BACK キーおよび FWRD キーで画面上のカーソル移動や数値の選択を行い，ENTR キーで決定します。例えばボードの close 処理を行いたい場合には，<Main Menu> で”Action”を選択して ENTR キーを押下し，続いて <ACTION> で”Close”を選択して ENTR キーを押下します。

4.1　メニュー

<Main Menu> 以下のメニュー構造を次の図に示します。メニューを操作していて，現在メニューのどの表示をしているか分からなくなった場合には，ENTR キーを何回か押下することで <Main Menu> に戻ることができます。また操作キーを操作せずに一定時間が経過しても <Main Menu> に戻ります。

図 4-1　メニュー構造

注※　待機系BCUでは操作できません

4.2 Line 情報の表示

Line の情報表示では，選択した Line 番号のインタフェース状態を表示します。

<INFORMATION> で”Line”を選択して ENTR キーを押下すると，NIF 番号選択画面が表示されます。

（1） NIF 番号選択

表示する Line の NIF 番号を選択する画面で FWRD キーを押していくと，選択可能な NIF 番号が昇順に表示されます。NIF が閉塞されている場合は，その NIF 番号の表示はスキップされます。BACK キーでは FWRD と逆の順序で NIF 番号が表示されます。情報表示したい NIF 番号を選択し，ENTR キーで決定すると Line 情報表示画面が表示されます。

図 4-2 NIF 番号選択の表示例

```
Ｗｈｉｃｈ ＮＩＦ？
  ＮＩＦ Ｎｏ． ◀００▶
```

（2） Line 情報表示

Line 情報表示画面では，物理インタフェースの状態を表示します。FWRD キーを押下すると，次の Line の情報を表示します。BACK キーでは，逆順となります。正常な NIF が複数存在する場合は，FWRD キーおよび BACK キーで NIF をまたいで Line 情報表示を行うこともできます。

ENTR キーを押下すると，<Main Menu> に戻ります。

図 4-3 Line 情報の表示例

```
０／１ ａｃｔｉｖｅ ｕｐ
１０００ＢＡＳＥ－ＳＸ ｆｕｌｌ
```

メッセージフォーマット
上段：NIF番号／Line番号，Line状態
下段：Line種別，全二重／半二重

表 4-1 Line 情報の表示内容

分類	名称	意味
Line 状態	active up	運用中 (正常動作中)
	active down	運用中 (回線障害発生中)
	initialize	初期化中またはネゴシエーション確立待ち
	test	回線テスト中
	fault	障害中
	closed	コマンド閉塞中
	unused	未使用 (コンフィグレーション未設定)
	mismatch	コンフィグレーション不一致
	locked	コンフィグレーションで閉塞中
	looped by remote	remote loopback テスト中

分類	名称	意味
	auto locked	回線テスト中のため自動で運用停止
Line 種別	10BASE-T	
	100BASE-TX	
	1000BASE-T	
	1000BASE-SX	
	1000BASE-LX	
	1000BASE-LH	
	10GBASE-SR	
	10GBASE-LR	
	10GBASE-ER	
	10GBASE-LW	
	10GBASE-EW	
	OC-192c/STM-64 POS(G.652-single-mode 2km)	
	OC-192c/STM-64 POS(G.652-single-mode 40km)	
	OC-48c/STM-16 POS(single-mode 2km)	
	OC-48c/STM-16 POS(single-mode 40km)	
全二重／半二重	full	全二重
	half	半二重
	full(auto)	全二重 (自動認識)
	half(auto)	半二重 (自動認識)

4.3 CPU 使用率の表示

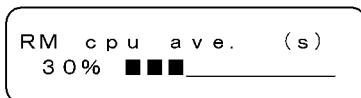
RM ボードおよび CP ボードの CPU 使用率を表示します。

<INFORMATION> で”CPU”を選択して ENTR キーを押下すると，CPU の使用率画面が表示されます。

(1) CPU 使用率

CPU 使用率を 2% 刻みの横棒グラフで表示します。表示は 1 秒ごとに最新の状況に更新されます。

図 4-4 CPU 使用率の表示例

```
ＲＭ　ｃｐｕ　ａｖｅ．　（ｓ）
 ３０％ ■■■___________
```

FWRD キーおよび BACK キーを押下するごとに，表示内容が次のように変わります。

（デフォルトの選択）→「RM cpu ave.(s)」→「CP cpu ave.(s)」→「RM cpu ave.(s)」

ENTR キーを押下すると，<Main Menu> に戻ります。

表 4-2 CPU 使用率の表示内容

表示項目	表示内容
RM cpu ave.(s)	RM の CPU 使用率を 1 秒単位で集計した平均値（%）
CP cpu ave.(s)	CP の CPU 使用率を 1 秒単位で集計した平均値（%）

4.4 メモリ使用率の表示

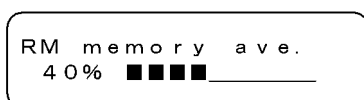
RM ボードのメモリ使用率および CP ボードのバッファ使用率を表示します。

<INFORMATION> で”Memory”を選択して ENTR キーを押下すると，メモリの使用率画面が表示されます。

(1) メモリ使用率

メモリ使用率を 2% 刻みの横棒グラフで表示します。表示は 1 秒ごとに最新の状況に更新されます。

図 4-5 メモリ使用率の表示例

```
RM memory ave.
 40% ■■■■________
```

FWRD キーおよび BACK キーを押下するごとに，表示内容が次のように変わります。

(デフォルトの選択) →「RM memory ave.」→「CP buff ave.(s)」→「RM memory ave.」

ENTR キーを押下すると，<Main Menu> に戻ります。

表 4-3 メモリ使用率の表示内容

表示項目	表示内容
RM memory ave.	RM での実装メモリの使用率（%）
CP buff ave.(s)	CP のバッファ使用率を 1 秒単位で集計した平均値（%）

4.5　バージョンの表示

本装置に組み込まれているソフトウェアと実装されているボードの情報を表示します。

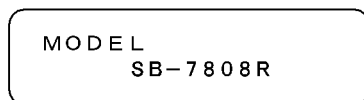
<INFORMATION> で”Ver”を選択して ENTR キーを押下すると，バージョン表示画面が表示されます。

（1）バージョン表示

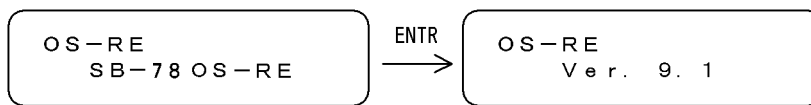
ボード型番の表示中に ENTR キーを押下すると，シリアルナンバーを表示できます（モデル名の表示中は除きます)。型番またはシリアルナンバーの表示中に FWRD キーを押下するごとに，表示するボードが次のように変わります。BACK キーでは逆順となります。

「モデル」→「SW」→「BCU0」→「BCU1」→「PRU0」→「PRU1」→・・・→「NIF0」→「NIF1」→・・・→「モデル」

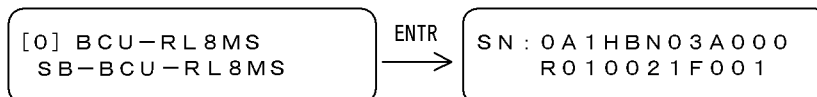
シリアルナンバーの表示中に ENTR キーを押下することにより，<Main Menu> に戻ります。モデル名またはボード型番の表示中は一度シリアルナンバーの表示になり，再度 ENTR キーを押下することにより，<Main Menu> メニューに戻ります。

図 4-6　バージョン表示の表示例（モデル）

ＭＯＤＥＬ
　　　　ＳＢ－７８０８Ｒ

メッセージフォーマット
上段：’ＭＯＤＥＬ’（固定）
下段：モデル名

図 4-7　バージョン表示の表示例（SW）

メッセージフォーマット
上段：ＳＷ略称
下段：ＳＷ型番

メッセージフォーマット
上段：ＳＷ略称
下段：ＳＷバージョン

図 4-8　バージョン表示の表示例（BCU）

メッセージフォーマット
上段：ボード番号，ボード略称
下段：ボード型番

メッセージフォーマット
上段：シリアルナンバー
下段：シリアルナンバー（続き）

4.6 シャーシ内温度の表示

BCU の温度情報を表示します。

<INFORMATION> で”Temp”を選択して ENTR キーを押下すると，温度表示画面が表示されます。

(1) 温度表示

FWRD キーを押下するごとに，表示するボードが次のように変わります。BACK キーでは逆順となります。

「BCU0」→「BCU1」→「BCU0」

ENTR キーを押下すると，<Main Menu> に戻ります。

図 4-9 温度表示の表示例

```
Ｔｅｍｐ：ＢＣＵ０
　　Ｎｏｒｍａｌ　２７℃
```

メッセージフォーマット
上段：Ｔｅｍｐ（固定），ボード種別
下段：温度のステータス，温度（℃）

表 4-4 温度のステータス

温度のステータス	表示内容
Normal	正常 (2 ℃～ 43 ℃)
Caution	注意 (～ 2 ℃，43 ℃～ 58 ℃)
Critical	警告 (58 ℃～ 65 ℃)

4.7　ボードの交換

電源を ON にしたまま，システム操作パネルからボードの交換を指示できます。交換できるボードは，次のとおりです。

待機系 BCU ボード，PRU ボード，NIF ボード

電源 ON したまま各ボードを交換する手順の概略は次のようになります。

1. システム操作パネルから close 指示を実行して，ボードを閉塞
2. 1. で閉塞させたボードの取り外し
3. 交換用ボードの取り付け
4. システム操作パネルから free 指示を実行して，ボードを運用再開

ボード交換の詳細な手順については「9　保守作業」を参照してください。

(1) ボード交換の選択

ボードを運用停止させる場合

<ACTION> で”CLOSE”を選択して ENTR キーを押下すると，close の操作が表示されます。

ボードを運用開始させる場合

<ACTION> で”FREE”を選択して ENTR キーを押下すると，free の操作が表示されます。

(2) 他の情報表示の抑制

ボードの交換の動作指示を行っている間は，障害情報の表示は行われません。

（3） close の操作

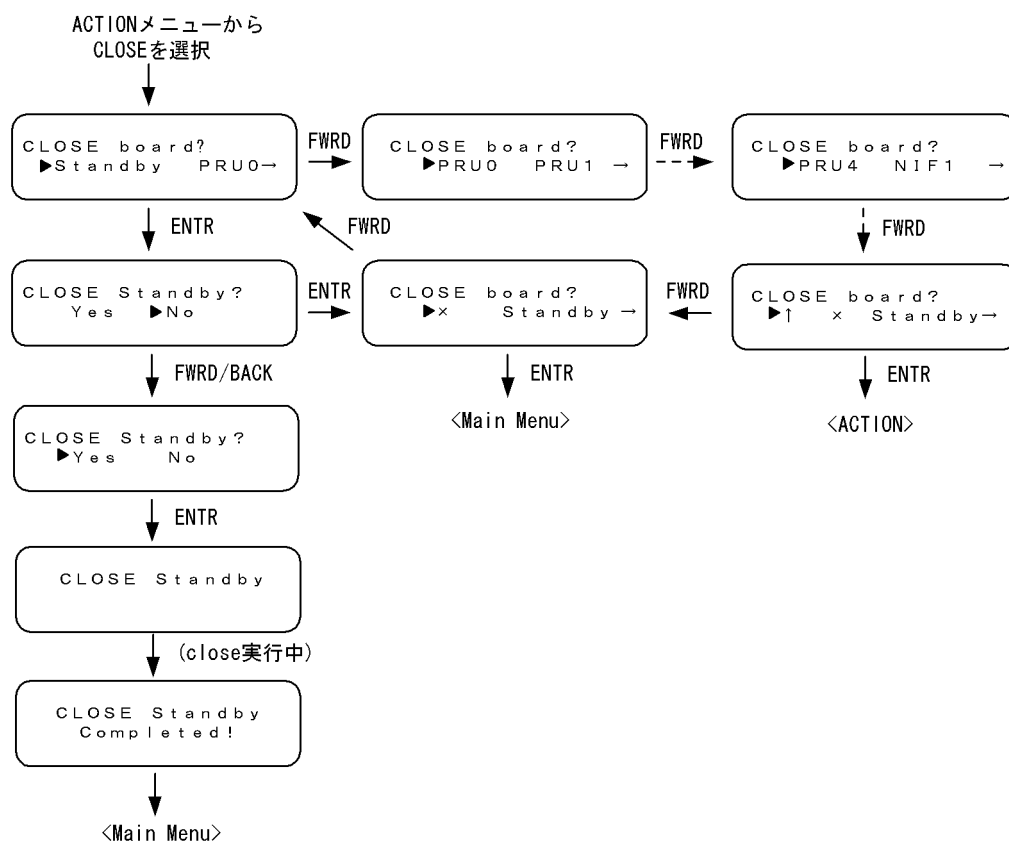
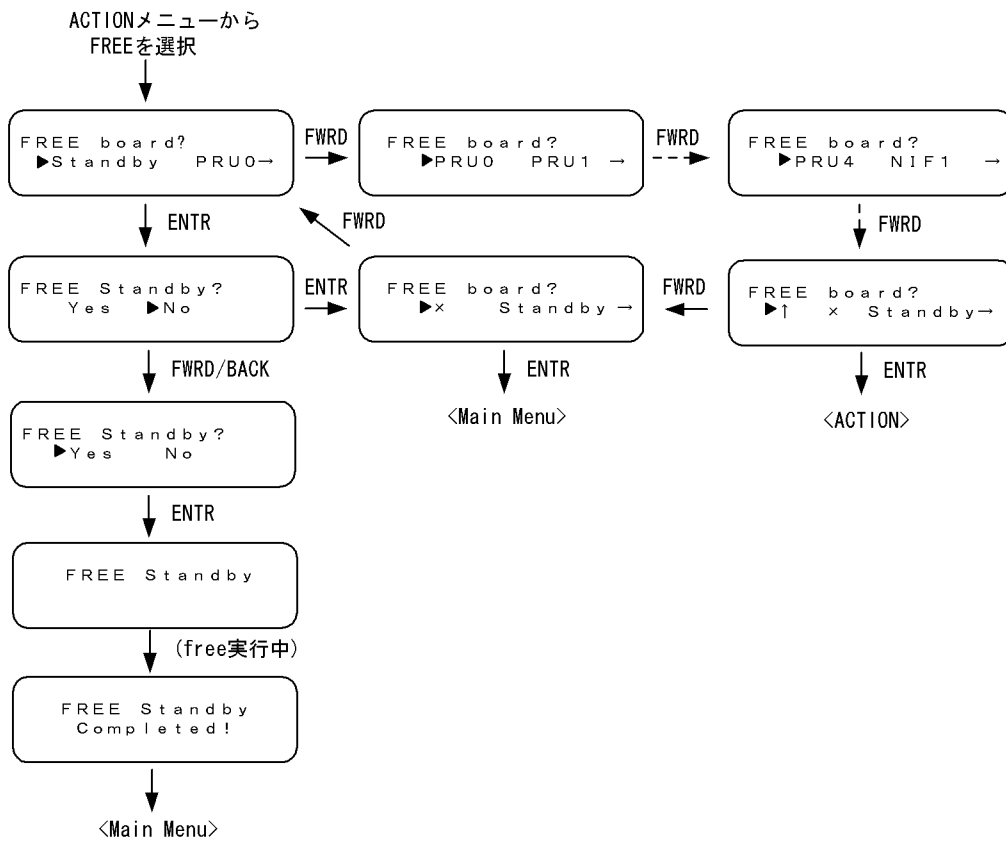
図 4-10　close の操作手順

（4） free の操作

図 4-11 free の操作手順

4.8 装置の停止

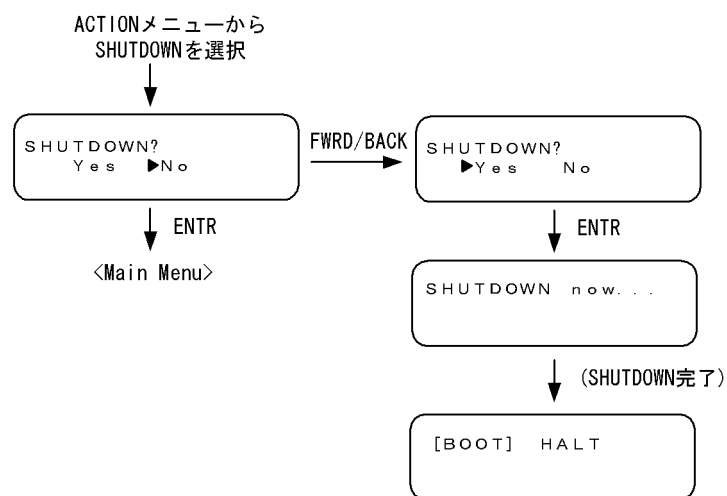
システム操作パネルから装置の停止を指示できます。システム操作パネルから装置を停止した場合，装置を再度起動する際は，電源スイッチで一度 OFF してから ON してください。

<ACTION> で”SHUTDOWN”を選択して ENTR キーを押下すると，装置の停止の操作が表示されます。

(1) 他の情報表示の抑制

装置の停止の動作指示を行っている間は，障害情報の表示は行われません。

(2) 装置の停止の操作

図 4-12 SHUTDOWN の操作手順

4.9 障害の表示

装置内で故障が発生した場合および装置内で故障が発生中に <Main Menu> から”Alarm”が選択された場合，故障部位または機能の切り分けを行うためにシステム操作パネルに障害表示を行います。BCU ボード上の ALARM LED が点灯している場合は，装置障害が発生していることを示す障害表示を行います。また，ERROR LED が点灯している場合は，装置の部分障害が発生していることを示す障害表示を行います。

障害表示は，エラーレベル E9，E8，E7，E6，E5 の障害に対して行われ，エラーレベルの高い障害が優先的に表示されます。障害個所が修復されると，障害表示は自動的に消えます。

(1) 障害表示の表示

障害が発生すると，エラーレベルとともにイベント発生部位とメッセージ ID がバックライトを点滅させながら表示されます。ENTR キーを押下すると，インタフェース識別子とその障害のメッセージテキストがバックライト点灯で表示されます。再度，ENTR キーを押下すると，<Main Menu> が表示されます。メッセージテキストは，画面左側に移動しながら繰り返し表示されます。

図 4-13 障害表示の表示例（NIF でハードウェア障害を検出した例）

メッセージID表示（デフォルト）

```
［Ｅ６］ ＮＩＦ
  Ｍｓｇ＝９０００２００１
```

バックライト点滅

ENTR →

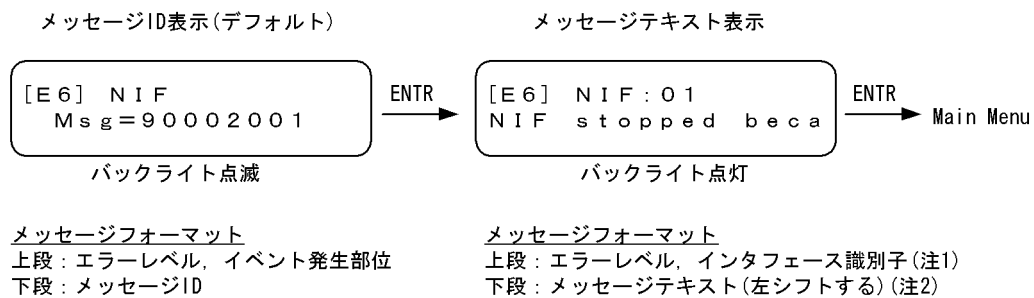
メッセージテキスト表示

```
［Ｅ６］ ＮＩＦ：０１
ＮＩＦ  ｓｔｏｐｐｅｄ  ｂｅｃａ
```

バックライト点灯

ENTR → Main Menu

メッセージフォーマット
上段：エラーレベル，イベント発生部位
下段：メッセージID

メッセージフォーマット
上段：エラーレベル，インタフェース識別子（注1）
下段：メッセージテキスト（左シフトする）（注2）

（注1） インタフェース識別子がないメッセージの場合は，イベント発生部位を示します。
（注2） 次のメッセージテキストが，左に1字ずつシフトしながら表示されます。
NIF Stopped because its hardware failure

(2) 障害表示中のメニューの表示

障害表示中，動作の指示を行うために <Main Menu> を表示するには，メッセージ ID 表示の場合は ENTR キーを 2 回，メッセージテキスト表示の場合は ENTR キーを 1 回押下します。

次の場合，メニュー表示から障害表示へ戻ります。

- 動作の指示以外の状態で，今まで表示していたエラーレベルよりも高い障害が発生した場合
- <Main Menu> で 10 秒間経った状態で，障害状態が解除されていない場合
- <Main Menu> から”Alarm”が選択された場合

(3) 他の情報表示との関係

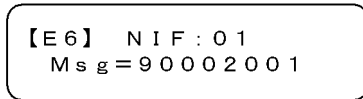
他の情報表示を行っている場合でも障害表示が優先して表示されます。ただし，動作の指示を行っている場合は，障害表示は行われません。動作の指示が終了した後，障害表示が行われます。

(4) 多重障害時の障害表示

多重障害が発生している場合は，エラーレベルを囲む括弧が【 】で表示されます。多重障害時には，

FWRD キーまたは BACK キーを押下するごとに，表示モードを維持しながら他の障害表示を順次行います。例えば，メッセージ ID 表示をしている場合は他のメッセージ ID 表示を行い，メッセージテキスト表示をしている場合は他のメッセージテキスト表示を行います。表示中の障害表示が発生している障害の中でエラーレベルが最上位のものでない場合は，表示してから 30 秒後にエラーレベルが最上位の障害表示に戻ります。

図 4-14　多重障害時の障害表示

```
【Ｅ６】　ＮＩＦ：０１
　Ｍｓｇ＝９０００２００１
```

5 初期導入時の作業

この章では，本装置を導入したときに必要な作業について説明しています。

5.1　ソフトウェアバージョンを確認する

運用開始後に，show version コマンドで本装置に組み込まれているソフトウェアの情報を確認してください。次の図に例を示します。

図 5-1　ソフトウェア情報の確認

```
SB-7800Rモデルの場合
> show version software
S/W: SB-78OS-R Ver. 9.2 [OS-R, Routing software]
>
```

また，二重化で本装置を運用する場合，運用系と待機系のソフトウェアバージョンが一致していることも確認してください。

図 5-2　ソフトウェア情報の確認（二重化運用時）

```
> show version
(途中省略)
BCU0/MC0: SB-78MC256 [MC256, 256MB compact flash memory card] 00070000
          SB-78OS-R Ver. 9.2 [OS-R, Routing software]
BCU0/MC1: ----------
          ----------
BCU1/MC0: SB-78MC256 [MC256, 256MB compact flash memory card] 00070000
          SB-78OS-R Ver. 9.2 [OS-R, Routing software]
BCU1/MC1: ----------
          ----------
>
```

5.2 ログインセキュリティを設定する

5.2.1 装置管理者モード移行のパスワードを設定する

コンフィグレーションコマンドを実行するためには enable コマンドで装置管理者モードに移行する必要があります。初期導入時に enable コマンドを実行した場合，パスワードは設定されていないので認証なしで装置管理者モードに移行します。ただし，通常運用中にすべてのユーザがパスワード認証なしで装置管理者モードに移行できるのはセキュリティ上危険なので，初期導入時にパスワードを設定しておいてください。次の図に実行例を示します。

図 5-3　初期導入直後の装置管理者モード移行のパスワード設定

```
> enable
# password
Changing local password for admin.
New password:
New password:
#
```

5.2.2 ログインユーザを作成する

adduser コマンドを用いて本装置にログインできるユーザを作成してください。次の図にログインユーザの作成例を示します。

図 5-4　ユーザ newuser を作成

また，RADIUS 認証を行う場合，RADIUS サーバに登録するユーザは本装置にも登録することをお勧めします。ただし，RADIUS サーバへの登録だけでもログインはできます。

5.2.3 初期導入時のログインユーザを削除する

初期導入時に設定されているログインユーザ”operator”を運用中のログインユーザとして使用しない場合は，セキュリティの低下を防ぐため，新しいログインユーザを作成したあとに rmuser コマンドで削除することをお勧めします。

5.2.4 同時にログインできるユーザ数を設定する

本装置に同時にログインできるユーザ数は，コンフィグレーションコマンド system で変更できます。次の図に設定例を示します。

図 5-5　同時にログインできるユーザ数の設定例

```
(config)# system login_user 5
(config)#
```

表 5-1　同時にログインできるユーザ数

時期	リモート運用端末（telnet，rlogin）
初期導入時	4
コンフィグレーション設定時	1 〜 10

同時ログインに関する動作概要を次に示します

- 複数ユーザが同時ログインを行うと，ログインしているユーザ数が制限数以下でもログインできない場合があります。
- モデムを使用したダイアルアップ IP 接続（「5.9　ダイアルアップ IP 接続を設定する」を参照）を行った場合，PPP コネクション用に接続しているユーザはログインユーザ・アカウント数には数えません。
- 同時にログインできるユーザ数を変更しても，すでにログインしているユーザのセッションが切れることはありません。
- コンソールや AUX ポートからのログインはユーザ数制限の対象とせず，ログインユーザ数にもカウントしません。

5.2.5　リモート運用端末からのログインを制限する

リモート運用端末から本装置へのログインについて，次に示す設定でログインを制限できます。なお，設定後はリモート運用端末から本装置へのログインの可否について確認してください。

（1） ログインを許可する IP アドレスを設定する

リモート運用端末から本装置にアクセスするには，コンフィグレーションコマンド system であらかじめアクセスを許可する端末の IP アドレスを登録しておく必要があります。アクセスを許可する IPv4 アドレスとサブネットマスク，または IPv6 アドレスとプレフィックスは，合わせて最大 128 個の登録ができます。なお，アクセスを許可していない（コンフィグレーションで登録していない）端末からのアクセスがあった場合，すでにログインしているその他の端末には，アクセスがあったことを示す”Unknown host address <IP アドレス >”のメッセージを表示します。

（2） プロトコル単位でログイン停止を設定する

本装置は，コンフィグレーションコマンド system で，リモート運用端末からのログインをプロトコル単位で停止できます。指定できるプロトコルは telnet，rlogin，および ftp です。

（3） RADIUS/TACACS+ を使用して認証する

リモート運用端末から本装置へのログイン時，RADIUS/TACACS+ を使用した認証が可能です。

5.2.6　CLI コマンドを制限する

RADIUS サーバもしくは TACACS+ サーバによる認証，またはローカル認証でログインしたユーザに対し，運用コマンドの制限（コマンド承認）を行うことができます。

コマンドの制限は，サーバから取得するコマンドクラスおよびコマンドリスト，またはコンフィグレーションで設定したコマンドクラスおよびコマンドリストに従って制御します。また，制限した運用コマンドは，CLI の補完機能では補完候補として表示しません。なお，パラメータの値や文字列自体がコマンドリストに設定された場合，補完候補表示は抑止しませんが，コマンド実行時には制限されます。

図 5-6　RADIUS/TACACS+ サーバによるログイン認証，コマンド承認

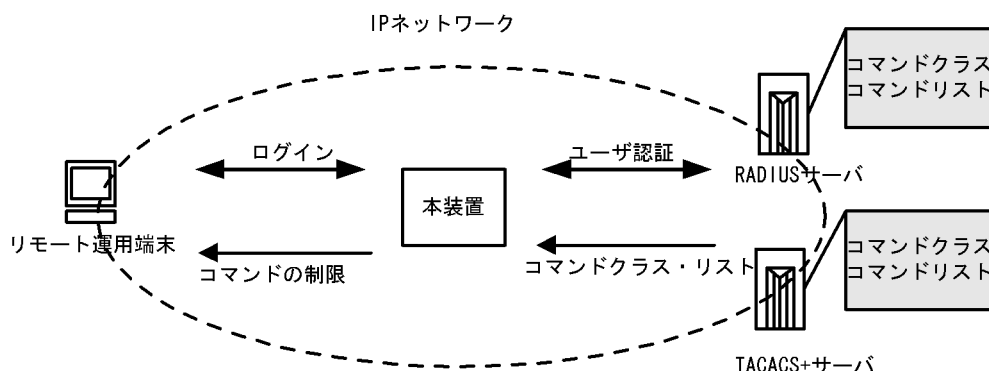
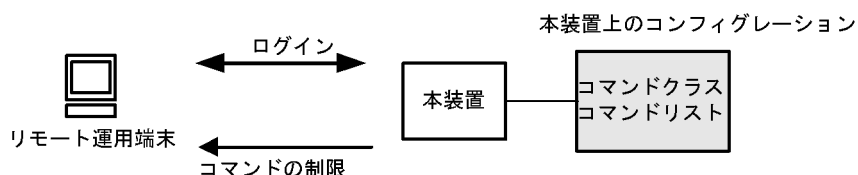



図 5-7　ローカルによるログイン認証，コマンド承認

RADIUS/TACACS+ によるコマンド承認を使用するためには，RADIUS/TACACS+ サーバおよび本装置を設定します。また，ローカルコマンド承認を使用するためには，本装置だけを設定します。

それぞれの設定手順を次に示します。

(1) コマンド制限のポリシーを決める

各ユーザに対し，運用コマンドの中で，制限・許可するコマンドのポリシーを決めます。ここでは，各ユーザがログインしたときに，あるコマンド群は許可し，それ以外のコマンドは制限するなどを決めます。ポリシーは「(2) リモート認証サーバまたはコンフィグレーションの設定をする」で RADIUS/TACACS+ サーバまたは本装置に設定します。

コマンド制限・許可の対象となるのは，運用コマンドです。/usr/local/diag/ 以下のコマンドなどの保守コマンド等は対象外で，常に制限されます（許可が必要な場合は，次に説明するコマンドクラスで "root" を指定してコマンド無制限クラスとしてください）。なお，logout, exit, quit, disable, end, set terminal, show whoami コマンドに関しては常に許可されます。また，コマンド承認時，旧シンタックス運用コマンドは常に制限されます。

本装置には，あらかじめ「コマンドクラス」として，以下のポリシーが定義されています。規定のコマンドクラスを選択することで，そのクラスの応じたコマンド制限を行うことができます。

表 5-2　コマンドクラス一覧

コマンドクラス	許可コマンド	制限コマンド
root 全コマンド無制限クラス※	従来どおりすべてのコマンド（保守コマンド等含む）	なし
allcommand 運用コマンド無制限クラス	すべての運用コマンド "all"	なし（保守コマンド等は不可）

コマンドクラス	許可コマンド	制限コマンド
noconfig コンフィグレーション変更制限クラス (コンフィグレーションコマンド投入も制限します)	制限以外の運用コマンド	"config, copy, erase startup-config, synchronize"
nomanage ユーザ管理コマンド制限クラス	制限以外の運用コマンド	"adduser, rmuser, clear password, password, killuser"
noenable 装置管理者モードコマンド制限クラス	制限以外の運用コマンド	"enable"

また，コマンドクラス以外に，許可コマンドリストと制限コマンドリストをそれぞれ指定することもできます。

注※　ただし，コマンドクラスに root を設定した場合，許可／制限コマンドリストの指定は無効となり，保守コマンド含むすべてのコマンドが投入可能になります。

(a)　コマンドリストの指定方法について

コマンドクラス以外に，許可／制限コマンドリストとして，許可コマンドと制限コマンドをそれぞれ指定できます。コマンドを指定する場合は，各コマンドリストに設定対象のコマンド文字列をスペースも意識して指定します。複数指定する場合はコンマ (,) で区切って並べます。ユーザのコマンド投入時に，コマンドリストで指定されたコマンド文字列と前方一致で判定されます。

なお，特別な文字列として，"all" を指定できます。"all" は運用コマンドすべてを意味します。

判定時に，許可コマンドリストと制限コマンドリストの両方に合致した場合は，合致したコマンド文字数が多い方の動作を採用します（ただし，"all" 指定は文字数を 1 とします）。その際，許可コマンドリストと制限コマンドリストに同じコマンド文字列が指定されていた場合は，許可として判定されます。

また，コマンドクラスと許可／制限コマンドリストを同時に指定した場合は，コマンドクラスごとに規定されているコマンドリスト（「表 5-2　コマンドクラス一覧」中の "" で囲まれているコマンドリストに対応）と許可／制限コマンドリストを合わせて判定を行います。なお，コマンドクラスに root を指定した場合，許可／制限コマンドクラスの設定は無効となり，保守コマンドを含むすべてのコマンドが投入可能になります。

例 1 ～ 7 にある各コマンドリストを設定した場合，本装置でどのようなコマンドが許可／制限されるかを示します。

(例 1)

許可コマンドリストだけを設定した場合，設定されたコマンドだけが投入を許可されます。

表 5-3　コマンドリスト例 1

コマンドリスト	投入コマンド	判定
許可コマンドリスト ="show ,ping" 制限コマンドリスト 設定なし	show ip route	許可
	ping ipv6 ::1	許可
	reload	制限

(例 2)

許可コマンドリストと制限コマンドリストの両方に合致した場合は，合致したコマンド文字数が多い方の動作とします (ただし，"all" 指定は文字数 1 とします)。

表 5-4　コマンドリスト例 2

コマンドリスト	投入コマンド	判定
許可コマンドリスト ="show ,ping ipv6" 制限コマンドリスト ="show ip,ping"	show system	許可
	show ipv6 route	制限
	ping ipv6 ::1	許可
	ping 10.10.10.10	制限

(例 3)

許可コマンドリストと制限コマンドリストの両方を設定し，両方に合致しない場合は，許可として判定されます。

表 5-5　コマンドリスト例 3

コマンドリスト	投入コマンド	判定
許可コマンドリスト ="show" 制限コマンドリスト ="reload"	ping 10.10.10.10	許可
	reload	制限

(例 4)

許可コマンドリストと制限コマンドリストに同じコマンド文字列が指定されている場合は，許可として判定されます。

表 5-6　コマンドリスト例 4

コマンドリスト	投入コマンド	判定
許可コマンドリスト ="show" 制限コマンドリスト ="show ,ping"	show system	許可
	ping ipv6 ::1	制限

(例 5)

コマンドリストを全く設定しなかった場合は，logout，exit，quit，disable，end，set terminal，および show whoami 以外のコマンドがすべて制限されます。

表 5-7　コマンドリスト例 5

コマンドリスト	投入コマンド	判定
許可コマンドリスト 設定なし 制限コマンドリスト 設定なし	logout, exit, quit, disable, end, set terminal, および show whoami 以外のコマンドすべて	制限
	logout, exit, quit, disable, end, set terminal, show whoami	許可

(例 6)

クラスとして root を指定した場合は，従来どおりすべてのコマンドが投入可能となります。なお，コマンドクラスに root を指定した場合，許可／制限コマンドクラスの制限は無効となり，保守コマンドを含むすべてのコマンドが投入可能となります。

表 5-8　コマンドリスト例 6

コマンドリスト	投入コマンド	判定
コマンドクラス ="root"	すべて (保守コマンド等含む)	許可

(例 7)

制限コマンドリストだけを設定した場合は，リストに合致しない運用コマンドはすべて許可となります。

表 5-9　コマンドリスト例 7

コマンドリスト	投入コマンド	判定
許可コマンドリスト 設定なし 制限コマンドリスト ="reload"	reload 以外の運用コマンドすべて	許可
	reload	制限

本マニュアルでは，例として次表のようなポリシーでコマンド制限を行います。

表 5-10　コマンド制限のポリシー例

ユーザ名	コマンドクラス	許可コマンド	制限コマンド
staff	allcommand	運用コマンドすべて	なし
guest	なし	制限以外の運用コマンドすべて許可	reload . . . ※ close . . . ※ enable . . . ※
test	なし	show ip . . . ※ (show ipv6 . . .　は制限)	許可以外，すべて制限

注※　. . . は任意のパラメータを意味します（show ip . . . は show ip route など）。

(2) リモート認証サーバまたはコンフィグレーションの設定をする

決定したコマンド制限ポリシーを基に，通常のログイン認証の設定以外に，RADIUS または TACACS+ のリモート認証サーバでは，以下の属性値を使用したコマンド制限のための設定を行います。ローカルコマンド承認では，コマンドクラスおよびコマンドリストのコンフィグレーションの設定をします。

なお，サーバまたはコンフィグレーションでコマンド承認の設定を行っていない場合，ユーザが認証されログインできても logout, exit, quit, disable, end, set terminal, show whoami 以外のすべてのコマンドが制限され，コマンドが投入できなくなるので注意してください。その場合は，コンソール端末からログインしてください。また，コマンド承認時，旧シンタックス運用コマンドは常に制限されます。

(a) RADIUS サーバを使用する場合

RADIUS サーバを利用してコマンド制限する場合は，認証時に以下のような属性値を返すようにサーバで設定します。

表 5-11　RADIUS 設定 Attribute 一覧

Type	Attribute	説明
25 Class	Class	クラス 次のどれかの文字列を一つ指定します。 root, allcommand, noconfig, nomanage, noenable

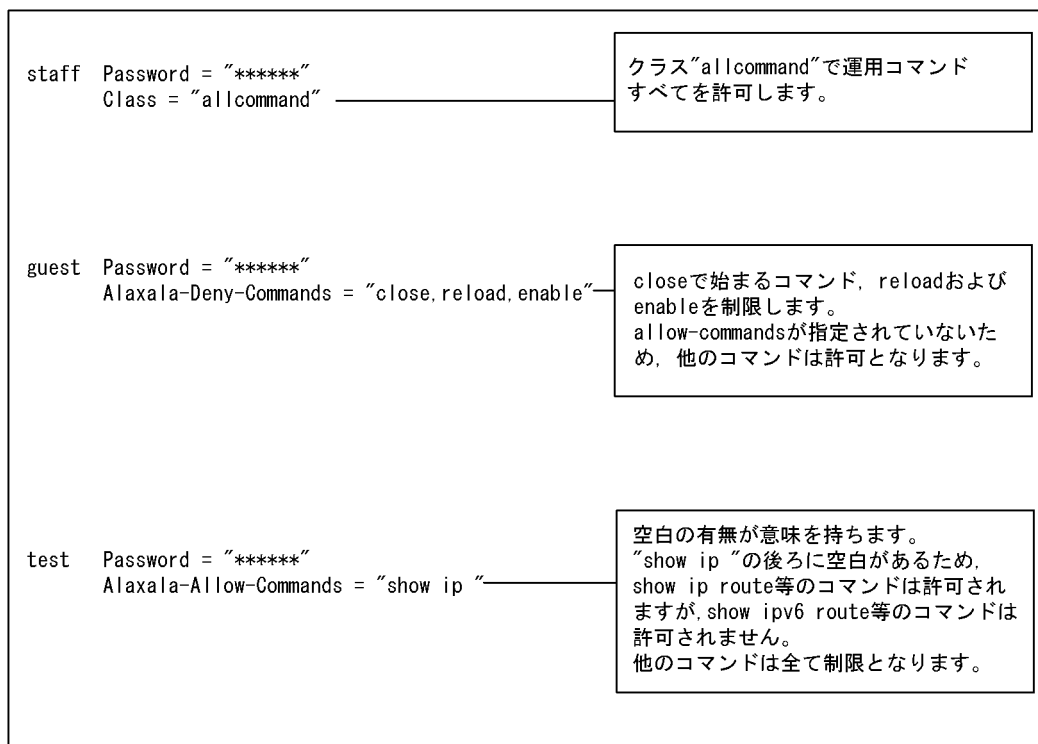
Type	Attribute	説明
26 Vendor-Specific Vendor-Id: 21839	ALAXALA-Allow-Commands Vendor type: 101	許可コマンドリスト 許可するコマンドの前方一致文字列をコンマ（,）で区切って指定します。空白も区別します。 運用コマンドすべては "all" を指定します。 許可コマンドリストだけ設定した場合は，許可コマンドリスト以外のコマンドはすべて制限となります。 （例：ALAXALA-Allow-Commands ="show ,ping ,telnet "）
	ALAXALA-Deny-Commands Vendor type: 102	制限コマンドリスト 制限するコマンドの前方一致文字列をコンマ（,）で区切って指定します。空白も区別します。 運用コマンドすべては "all" を指定します。 制限コマンドリストだけ設定した場合は，制限コマンドリスト以外はすべて許可となります。 （例：ALAXALA-Deny-Commands="enable,reload,close"）

RADIUS サーバでは上記のベンダー固有属性をサポートしていない場合があります。その場合は，サーバに上記のベンダー固有属性を登録（dictionary ファイルなどに設定）してください。

図 5-8　RADIUS サーバでのベンダー固有属性の dictionary ファイル登録例

```
VENDOR          Alaxala                      21839
ATTRIBUTE       Alaxala-Allow-Commands       101       string  Alaxala
ATTRIBUTE       Alaxala-Deny-Commands        102       string  Alaxala
```

「表 5-10　コマンド制限のポリシー例」で決定したポリシーを一般的な RADIUS サーバに設定する場合，以下のようなイメージになります。

図 5-9　RADIUS サーバ設定例

注 ******の部分には各ユーザのパスワードを設定します。

注意事項

- 本装置では Class エントリを複数受信した場合，1 個目の Class を認識し 2 個目以降の Class エントリは無効となります。

図 5-10　複数 Class エントリ設定例

```
Class = "noenable"
Class = "allcommand"
```

本装置では1個目のnoenableだけ有効となります。

- 本装置では Class エントリに複数のクラス名を記述した場合，1 個目のクラス名を認識し 2 個目以降のクラス名は無効となります。例えば class="nomanage,noenable" と記述した場合，nomanage だけが有効になります。
- Alaxala-Deny-Commands, Alaxala-Allow-Commands のそれぞれにおいて，同一属性のエントリを複数受信した場合，一つの属性につきコンマ (,）と空白も含み 1024 文字までを認識し，1025 文字以降は受信しても無効となります。なお，下記の例のように同一属性を複数エントリ記述し，本装置で 2 個目以降のエントリを受信した場合にはエントリの先頭に自動的にコンマ (,）を設定します。

図 5-11　複数 Deny-Commands エントリ設定例

(b) TACACS+ サーバを使用する場合

TACACS+ サーバを使用してコマンド制限する場合は，TACACS+ サーバで承認の設定として以下のような属性 - 値のペアを設定します。

表 5-12　TACACS+ 設定 Attribute-Value 一覧

Service	Attribute	Value
grlogin	class	クラス 次のどれかの文字列を指定 root, allcommand, noconfig, nomanage, noenable
	allow-commands	許可コマンドリスト 許可するコマンドの前方一致文字列をコンマ（,）で区切って指定します。空白も区別します。 運用コマンドすべては "all" を指定します。 許可コマンドリストだけ設定した場合は，許可コマンドリスト以外のコマンドはすべて制限となります。 （例：allow-commands="show ,ping ,telnet "）

Service	Attribute	Value
	deny-commands	制限コマンドリスト 制限するコマンドの前方一致文字列をコンマ（,）で区切って指定します。空白も区別します。 運用コマンドすべては "all" を指定します。 制限コマンドリストだけ設定した場合は，制限コマンドリスト以外はすべて許可となります。 （例：deny-commands="enable,reload,close"）

「表 5-10　コマンド制限のポリシー例」で決定したポリシーを一般的な TACACS+ サーバに設定する場合，以下のような設定ファイルイメージになります。

図 5-12　TACACS+ サーバ設定例

```
user=staff {
    login = cleartext "******"
    service = grlogin {
        class = "allcommand"
    }
}

user=guest {
    login = cleartext "******"
    service = grlogin {
        deny-commands = "reload,close,enable"
}

user=test {
    login = cleartext "******"
    service = grlogin {
        allow-commands = "show ip "
}
```

service名はgrloginと設定します。
クラス"allcommand"で運用コマンドすべてを許可します。

reload，closeまたはenableで始まるコマンドを制限します。
allow-commandsが指定されていないため，他のコマンドは許可となります。

空白の有無が意味を持ちます。
「show ip」の後ろに空白があるため，show ip route等のコマンドは許可されますが，show ipv6 route等のコマンドは許可されません。
他のコマンドはすべて制限となります。

注　******の部分は各ユーザのパスワードを設定します。

注意事項

- 本装置では class エントリに複数のクラス名を記述した場合，1 個目のクラス名を認識し 2 個目以降のクラス名は無効となります。例えば class="nomanage,noenable" と記述した場合，nomanage だけが有効になります。
- deny-commands, allow-commands のそれぞれにおいて，一つの属性につきコンマ（,）と空白も含み 1024 文字までを認識し，1025 文字以降は受信しても無効となります。

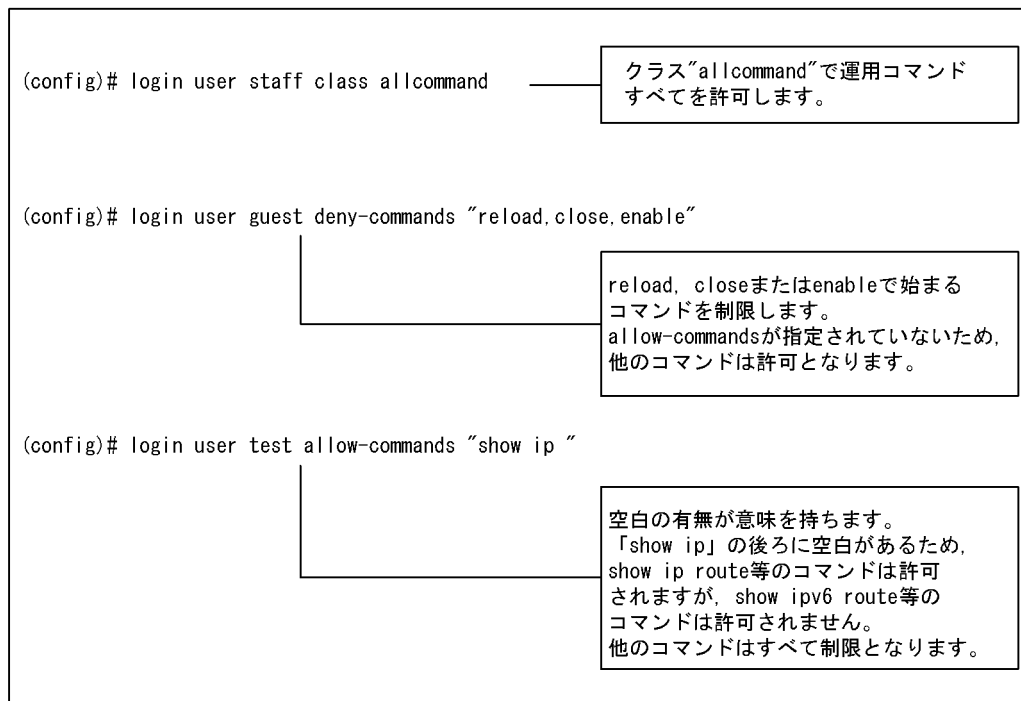
(c) ローカルコマンド承認を使用する場合

ローカルコマンド承認を使用してコマンド制限する場合は，ログインコンフィグレーション（login コマンド）でユーザ名を指定して，各パラメータで以下のようなコンフィグレーションを設定します。

表 5-13　ローカルコマンド承認使用時のコマンドクラスおよびコマンドリスト設定一覧

パラメータ	説明
class	クラス 次のどれかを指定 root，allcommand，noconfig，nomanage，noenable
allow-commands	許可コマンドリスト 許可するコマンドの前方一致文字列をコンマ（,）で区切って指定します。空白も区別します。 運用コマンドすべては "all" を指定します。 許可コマンドリストだけ設定した場合は，許可コマンドリスト以外のコマンドはすべて制限となります。 （例：(config)# login user staff allow-commands "show ,ping ,telnet"）
deny-commands	制限コマンドリスト 制限するコマンドの前方一致文字列をコンマ（,）で区切って指定します。空白も区別します。 運用コマンドすべては "all" を指定します。 制限コマンドリストだけ設定した場合は，制限コマンドリスト以外はすべて許可となります。 （例：(config)# login user staff deny-commands "enable,reload,close"）

「表 5-10　コマンド制限のポリシー例」で決定したポリシーをコンフィグレーションに設定する場合，以下のような設定イメージになります。

図 5-13　コンフィグレーションの設定例

(3)　本装置のログイン認証・コマンド承認を設定する

RADIUS/TACACS+ サーバを使用する場合，サーバ側の設定が終了した後，本装置で RADIUS または TACACS+ サーバのコンフィグレーション設定を行います。RADIUS サーバまたは TACACS+ サーバのアドレス，共有鍵などのサーバ設定とコマンド承認を行うパラメータ（authorization）設定を行ってください。

ローカルコマンド承認を使用する場合，コマンドクラスおよびコマンドリストの設定が終了した後，ログインコンフィグレーション（login コマンド）でコマンド承認を行うパラメータ（authorization）を設定

してください。

なお，サーバまたはコンフィグレーションで「(2) リモート認証サーバまたはコンフィグレーションの設定をする」のコマンド承認の設定がされていない場合は，authorization を設定した装置にユーザが認証されログインしても，コマンドがすべて制限されるため，コマンドの投入はできません。設定ミス等でコマンド投入できない場合は，コンソール端末からログインして修正してください。

図 5-14　RADIUS サーバを使用する場合

```
(config)# radius 192.168.10.1 key "RaD#001"
(config)# radius authorization
(config)# show radius

       radius yes
       radius authorization
       radius 192.168.10.1 key "RaD#001"
```

サーバの IP アドレス (例では 192.168.10.1)，共有鍵（例では RaD#001）は，ご利用の環境にあわせて設定してください。

図 5-15　TACACS+ サーバを使用する場合

```
(config)# tacacs+ 192.168.10.1 key "TaC#001"
(config)# tacacs+ authorization
(config)# show tacacs+

       tacacs+ yes
       tacacs+ authorization
       tacacs+ 192.168.10.1 key "TaC#001"
```

サーバの IP アドレス (例では 192.168.10.1)，共有鍵（例では TaC#001）は，ご利用の環境にあわせて設定してください。

図 5-16　ローカルコマンド承認を使用する場合

```
(config)# login authorization
(config)# show login

       login authorization                                 ┐
       login user guest deny-commands "reload,close,enable" │※
       login user staff class allcommand                   │
       login user test allow-commands "show ip "           ┘
```

注※　「表 5-10　コマンド制限のポリシー例」で決定したポリシーをローカルコマンド承認で設定した場合，このようなコンフィグレーションとなります。

最後に，RADIUS，TACACS+ またはローカルの認証方式の設定を行います。その他，通常のリモートアクセスに必要な設定は，あらかじめ行ってください。

図 5-17　RADIUS サーバを使用する場合

```
(config)# system login_authentication radius local
```

図 5-18　TACACS+ サーバを使用する場合

```
(config)# system login_authentication tacacs+ local
```

図 5-19　ローカルコマンド承認を使用する場合

```
(config)# system login_authentication local
```

（4） ログインしての確認

設定が完了した後，RADIUS/TACACS+/ ローカル認証を使用したリモート運用端末から本装置へのログインを行います。ログイン後，show whoami コマンドでコマンドリストが設定されていること，コマンドを投入して制限・許可していることを確認してください。

図 5-20 staff がログイン後の確認例

```
> show whoami
staff: ttyp0    ----- 2  Aug 6 14:17:03(10.10.10.10)

Home-directory: /usr/home/staff
Authentication: TACACS+ (Server 192.168.10.1)
Class: allcommand
      Allow: "all"
      Deny : -----
Command-list: -----
>
> show cal
Wed Oct 29 17:21:15  2003
> /bin/date
% Command not authorized.
>
```

図 5-21 guest がログイン後の確認例

```
>show whoami
guest: ttyp0    ----- 2  Aug 6 14:17:03(10.10.10.20)

Home-directory: /usr/home/guest
Authentication: RADIUS (Server 192.168.10.1)
Class: -----
Command-list:
      Allow: -----
      Deny : "reload,close,enable"
>
> show cal
Wed Oct 29 17:21:15  2003
> reload
% Command not authorized.
>
```

図 5-22 test がログイン後の確認例

```
>show whoami
test: ttyp0    ----- 2  Aug 6 14:17:03(10.10.10.30)

Home-directory: /usr/home/test
Authentication: LOCAL
Class: -----
Command-list:
      Allow: "show ip "
      Deny : -----
>
> show ip route
***コマンド実行されます***
> show ipv6 route
% Command not authorized.
>
```

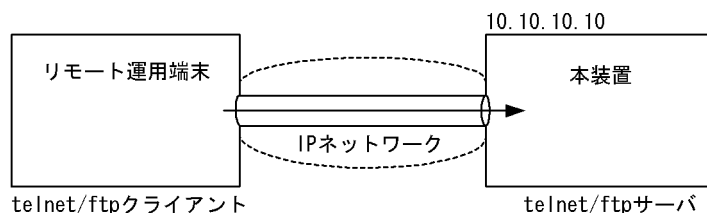
5.2.7 ログイン前にメッセージを表示する

（1） 概要

コンフィグレーションでログイン前メッセージの設定を行うと，リモート運用端末の telnet や ftp クライアントから本装置に接続したとき，ログインする前にメッセージを表示します。

(2) 構成図と条件

リモート運用端末の telnet や ftp クライアントからネットワークを介して本装置の telnet や ftp サーバへ接続する構成とします。

図 5-23 telnet や ftp で接続する構成

設定条件

1. サーバ・クライアント間の通信設定や本装置でのリモートアクセス設定は完了しているものとします。
2. コンフィグレーションで設定する以下のメッセージを，接続してきたユーザに対してログイン前に表示します。

```
##########################################
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.
##########################################
```

(3) 本装置のログイン前メッセージを設定する

本装置でログイン前メッセージのコンフィグレーション設定を行います。

図 5-24　system login_message before-login を設定する

(4) 接続してログイン前にメッセージを表示する

設定が完了したら，リモート運用端末の telnet/ftp クライアントから本装置へ接続します。接続後，クライアントにメッセージが表示されます。

図 5-25　リモート運用端末から本装置へ接続した例

●telnetで接続した場合

```
> telnet 10.10.10.10
Trying 10.10.10.10...
Connected to 10.10.10.10.
Escape character is '^]'.

###########################################
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.
###########################################
login:
```

●ftpで接続した場合

```
> ftp 10.10.10.10
Connected to 10.10.10.10.
220-###########################################
220-Warning!!! Warning!!! Warning!!!
220-This is our system. You should not login.
220-Please close connection.
220-###########################################
220 FTP server (Version wu-2.4(1) Fri Aug 27 15:15:05 JST 2004) ready.
Name (10.10.10.10:staff):
```

(5) 注意事項

- ログインメッセージに設定できる文字数は英数字で最大 720 文字（エンコード後は最大 960 文字）です。
- ログインメッセージを入力する際には，クライアントの画面設定を確認し，表示できない文字を入力しないでください。show system login_message [before-login | after-login | before-login-ftp | after-login-ftp] plain-text 実行時や，クライアント接続時に画面やプロンプトの表示が崩れ，操作できなくなる恐れがあります。
- クライアントへの問い合わせプロンプトが不要なログインをした場合（クライアント側が自動的にユーザ名を渡す場合でパスワードが不要な場合や，rlogin 認証でパスワード問い合わせが不要な場合など）は，ログインメッセージと認証後の画面が続けて表示されます。

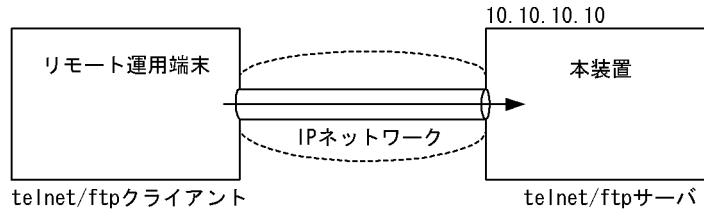
5.2.8 ログイン後にメッセージを表示する

(1) 概要

コンフィグレーションでログイン後メッセージの設定を行うと，リモート運用端末の telnet や ftp クライアントから本装置に接続したとき，ログインした後にメッセージを表示します。なお，本設定では ftp のログイン後メッセージは表示させないことにします。

(2) 構成図と条件

リモート運用端末の telnet や ftp クライアントからネットワークを介して本装置の telnet や ftp サーバへ接続する構成とします。

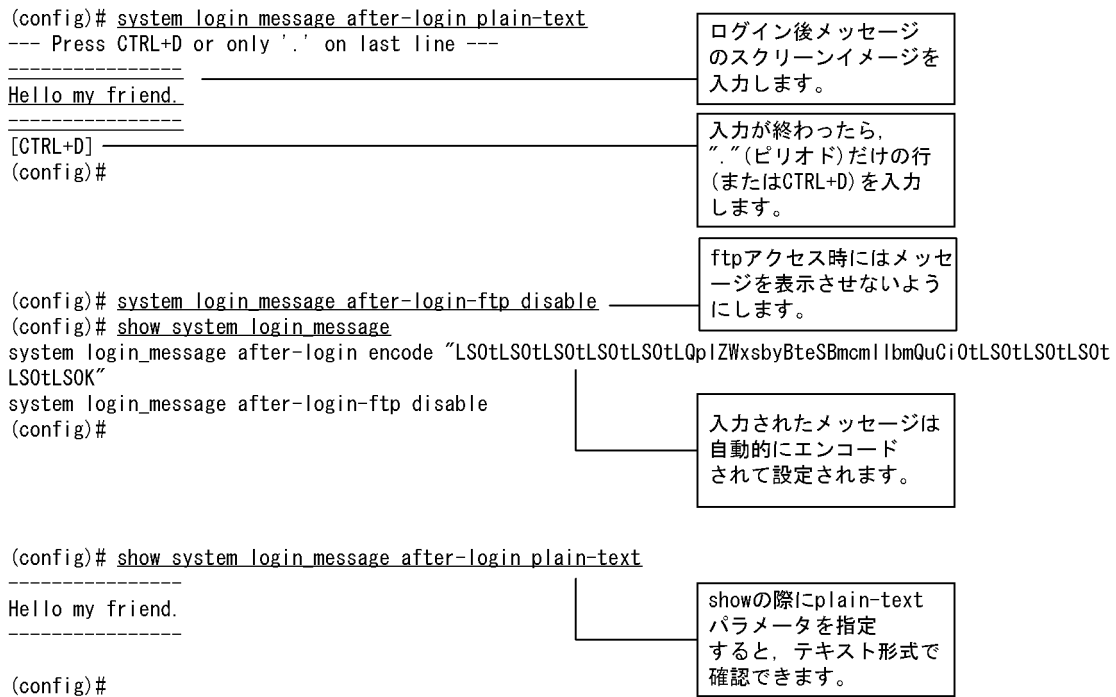
図 5-26 telnet や ftp で接続する構成

設定条件

1. サーバ・クライアント間の通信設定や本装置でのリモートアクセス設定は完了しているものとします。
2. コンフィグレーションで設定する以下のメッセージを，接続してきたユーザに対してログイン後に表示します。なお，本設定では ftp アクセスの場合には表示させません。

```
----------------
Hello my friend.
----------------
```

(3) 本装置のログイン後にメッセージを設定する

本装置でログイン後，メッセージのコンフィグレーション設定を行います。

図 5-27　system login_message after-login を設定する

(4) 接続してログイン後メッセージを確認する

設定が完了したら，リモート運用端末の telnet/ftp クライアントから本装置へ接続します。認証ログイン後，telnet クライアントにメッセージが表示され，ftp クライアントでは表示されません。

図 5-28 リモート運用端末から本装置へ接続した例

●telnetで接続した場合

```
> telnet 10.10.10.10
Trying 10.10.10.10...
Connected to 10.10.10.10.
Escape character is '^]'.

login: staff
Password: ******
Copyright (c) 2005 Allied Telesis Holdings K.K. All rights reserved.

----------------
Hello my friend.
----------------
*** Welcome to the System ***
>
```

●ftpで接続した場合

```
> ftp 10.10.10.10
Connected to 10.10.10.10.
221 FTP server (Version wu-2.4(1) Fri Aug 27 15:15:05 JST 2004) ready.
Name (10.10.10.10:staff):
331 Password required for staff.
Password: ******
230 User staff logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

(5) 注意事項

- ログインメッセージに設定できる文字数は英数字で最大 720 文字(エンコード後は最大 960 文字)です。
- ログインメッセージを入力する際には,クライアントの画面設定を確認し,表示できない文字を入力しないでください。show system login_message [before-login | after-login | before-login-ftp | after-login-ftp] plain-text 実行時や,クライアントのログイン後に画面やプロンプトの表示が崩れ,操作できなくなる恐れがあります。

5.3　時刻を設定する

5.3.1　概要

時刻は，本装置のログ情報や各種ファイルの作成時刻などに付与される情報です。運用開始時には正確な時刻を本装置に設定してください。時刻は，set calendar コマンドで設定します。

また，このほかに時刻情報に関連する設定には次の表に示すコマンドや機能があります。

表 5-14　時刻情報に関連する設定

項番	コマンド／機能	設定内容	参照先
1	config system コマンドの timezone パラメータ	装置のタイムゾーンを設定します。	「コンフィグレーションコマンドレファレンス Vol.1　system」
2	NTP 機能	NTP プロトコルにより時刻情報を NTP サーバに同期させます。	「コンフィグレーションコマンドレファレンス Vol.2　ntp（NTP 情報）」
3	rdate コマンド	リモートから日付・時刻情報を取得し設定します。	「運用コマンドレファレンス Vol.1　rdate」

5.3.2　時刻変更に関する注意事項

- 本装置で収集している統計情報の RM および CP の CPU 使用率と CP のバッファ使用率は，時刻が変更された時点で 0 クリアされます。
- OSPF，OSPFv3，IS-IS 使用時，時刻補正を HelloInterval 時間（デフォルト 10 秒）内に連続して実行（(RouterDeadInterval 時間 - HelloInterval 時間) / 3 回以上（デフォルトは 30/3=10 回以上)）した場合，隣接関係が切断されることがあります。
- スタティック経路の動的監視機能の連続失敗回数を 1 回で使用したとき，現在時刻より 3 秒以上進めた場合，該当経路を使用した通信が一時的に切断されることがあります。
- BGP4，BGP4+ を使用したとき，時刻補正を HoldTime 内に連続して実行（連続時刻補正回数× 10 秒 > HoldTime）した場合，隣接関係が切断されることがあります。また，HoldTime を 10 秒以下で使用した場合，1 回の時刻補正で隣接関係が切断されることがあります。

5.4　NIF ボードを実装する

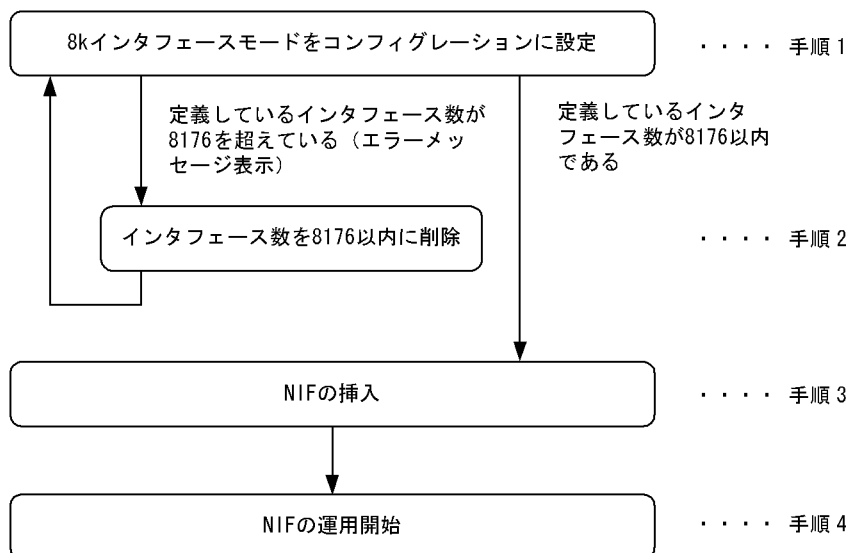
5.4.1　NE1G-48T の実装手順

(1)　実装手順

以下の NIF ボード※を実装する場合，インタフェースモードを 8k インタフェースモードに設定する必要があります。16k インタフェースモードがスタートアップコンフィグレーションファイルに設定されている場合，コンフィグレーション不一致により運用できません。以下の NIF ボード※を実装する概略手順を次の図に示します。

注※　実装する NIF ボード

- NE1G-48T

図 5-29　実装手順

インタフェースモードの設定手順の詳細説明を記載します。

(手順 1）8k インタフェースモードをコンフィグレーションに設定

8k インタフェースモードをコンフィグレーションに設定します。設定方法については「コンフィグレーションガイド　5.1.1 NE1G-48T を実装する」を参照してください。

(手順 2）インタフェース数を 8176 以内に削除

定義しているインタフェース数を 8176 以内に削除します。削除後，再度，(手順 1）から実施してください。

(手順 3）NIF の挿入

NIF の空きスロットに NIF ボードを挿入します。挿入方法の詳細については，「ハードウェア取扱説明書」を参照してください。

〔注意事項〕

感電する恐れがあります。電源を ON したままでのボードの取り外し／取り付け作業は，教育を受けた技術者または保守員にご依頼ください。

（手順 4）NIF の運用開始

挿入した NIF ボードを運用状態にします。NIF ボードが接続されている PRU ボードが運用状態の場合，次に示す free nif コマンドを運用端末から実行します。

```
free nif <NIF No.>[Enter]     (NIF No.：対象となるNIF番号)
```

PRU ボードが停止状態の場合，次に示す free pru コマンドを運用端末から実行します。PRU の運用開始と共に，NIF ボードは運用開始されます。

```
free pru<PRU No.>[Enter]     (PRU No.：対象となるPRU番号)
```

（2） インタフェースモード変更時の注意事項

装置起動後，インタフェース数を 8176 より多く定義したことがある場合，インタフェースモードを 16k インタフェースモードから 8k インタフェースモードに変更すると本装置の再起動が必要となることがあります。

（3） BCU 二重化運用中にインタフェースモード変更したときの注意事項

BCU 二重化構成で装置起動後，インタフェース数を 8176 より多く定義したことがある場合，インタフェースモードを 16k インタフェースモードから 8k インタフェースモードに変更すると本装置の再起動が必要となることがありますが，再起動を行うと運用系・待機系共に再起動を行います。

5.5 ボードの実装状態を確認する

装置起動後は，実装した BCU/PRU/NIF ボードの動作状態や搭載メモリ量などを確認してください。また，本装置はボードの種類が限定される機能もあります（詳細は「解説書 Vol.1　3. 収容条件」を参照）ので，スタートアップコンフィグレーションファイルを設定する前には，ボードの種類も確認してください。

（1） BCU/PRU ボード

BCU/PRU ボードの状態や種類は show system コマンドで確認してください。

図 5-30　BCU/PRU ボードの確認（1/2）

```
> show system
2003/01/11 19:30:15
System : SB-7808R-AC, SB-78OS-R Ver. 9.2 [OS-R]
Node : Name=System Name
    Contact=Contact Address
    Locate=Location
    Node Info : Duplex Mode
    Elapsed Time : 00:01:35
    PRU-Resource : router-b1
    IP Routing Entry :
        Unicast : current number=5 , max number=256000
        Multicast : current number=5 , max number=8192
        ARP : current number=2 , max number=128000
    IPv6 Routing Entry :
        Unicast : current number=2 , max number=32000
        Multicast : current number=5 , max number=8192
        NDP : current number=2 , max number=32000
    FAN : Active No=FAN0(1),FAN0(2),FAN0(3),FAN1(4),FAN1(5),FAN1(6) Speed=Normal
    POW0 : Active
    POW1 : Active
    POW2 : Disconnect
    POW3 : Disconnect
    BCU0 : Active
        RM-CPU : Active SB-BCU-RM8MS [BCU-RM8MS] 0000
        Boot : 2003/01/11 19:27:42 , Power ON , 0 times restart
        Lamp : ACTIVE LED=green , READY LED=green ,
            EMA SUPPRESS LED=light off , ALARM LED=light off ,
            ERROR LED=light off
        SYSTEM OPERATION PANEL : No error
        Board : CPU=Intel Pentium 3 850MHz , Memory=262,144kB(256MB)
        Temperature : Normal(27degree)
        RM Ether : unused
        CP-CPU : Active
            Boot : 2003/10/11 19:27:42 , Power ON , 0 times restart
            Board : CPU=RM5261 250MHz , Memory=262,144kB(256MB)
        MC0 : Primary Slot , MC-Enabled
            SB-78MC256[MC256] , SB-7800R Format , 00070000
            29,563kB used (User Area: 29,563kB , Dump Area: 0kB)
            200,181kB free (User Area: 176,181kB , Dump Area: 24,000kB)
            229,744kB total(User Area: 205,744kB , Dump Area: 24,000kB)
        MC1 : Secondary Slot , MC-Disconnect
    BCU1 : Standby
        RM-CPU : Active SB-BCU-RM8MS [BCU-RM8MS] 0000
        Boot : 2003/01/11 19:27:43 , Power ON , 0 times restart
        Lamp : ACTIVE LED=light off , READY LED=green ,
        EMA SUPPRESS LED=light off , ALARM LED=light off ,
        ERROR LED=light off
        SYSTEM OPERATION PANEL : No error
        Board : CPU=Intel Pentium 3 850MHz , Memory=262,144kB(256MB)
        Temperature : Normal(28degree)
        CP-CPU : Active
            Boot : 2003/01/11 19:27:43 , Power ON , 0 times restart
            Board : CPU=RM5261 250MHz , Memory=262,144kB(256MB)
```

図 5-31　BCU/PRU ボードの確認（2/2）

```
        MC0 : Primary Slot , MC-Enabled
            SB-78MC256[MC256] , SB-7800R Format , 00070000
            29,563kB used (User Area: 29,563kB , Dump Area: 0kB)
            200,181kB free (User Area: 176,181kB , Dump Area: 24,000kB)
            229,744kB total(User Area: 205,744kB , Dump Area: 24,000kB)
        MC1 : Secondary Slot , MC-Disconnect
    PRU0 : Active SB-PRU-B2 [PRU-B2]
        Lamp : LED=green
        Memory : size=131,072kB(128MB)
        FDB : current number=2 , max number=128000
    PRU1 : Active SB-PRU-B2 [PRU-B2]
        Lamp : LED=green
        Memory : size=131,072kB(128MB)
        FDB : current number=2 , max number=128000
    PRU2 : Disconnect
    PRU3 : Disconnect
>
```

（2） NIF ボード

NIF ボードの状態や種類は show nif コマンドで確認してください。なお，show nif コマンドで表示される NIF 番号と対応する PRU 番号は次の表に示すとおり，装置モデル別に異なるので注意してください。

表 5-15　NIF と PRU の実装関係

モデル	NIF 番号	PRU 番号
SB-7804R	0 ～ 1	0
	2 ～ 3	1
SB-7808R	0 ～ 1	0
	2 ～ 3	1
	4 ～ 5	2
	6 ～ 7	3
SB-7816R	0 ～ 1	0
	2 ～ 3	1
	4 ～ 5	2
	6 ～ 7	3
	8 ～ 9	4
	10 ～ 11	5
	12 ～ 13	6
	14 ～ 15	7

5.6　コンフィグレーションを設定する

5.6.1　概要

運用開始時，本装置に接続するネットワークのメディアの種類や使用するルーティングプロトコルなど，本装置の動作環境をコンフィグレーションに定義してください。コンフィグレーションは，コンフィグレーションコマンドで定義できます。個々のコンフィグレーションの説明やコマンド，パラメータの仕様については「コンフィグレーションコマンドレファレンス Vol.1」「コンフィグレーションコマンドレファレンス Vol.2」を参照してください。また「コンフィグレーションガイド」に，スタートアップコンフィグレーションファイルおよびバックアップコンフィグレーションファイルの運用方法やコンフィグレーションの設定操作例を掲載しているので，併せて参照してください。

5.6.2　二重化運用時の注意事項

本装置を二重化で運用している場合，装置起動時とコンフィグレーション設定時に運用系と待機系のコンフィグレーションファイルが同じであるかどうかのチェックを行います。もし運用系と待機系のコンフィグレーションファイルが異なっている場合には，

```
E3 CONFIG 00010005 0100:000000000000 There is mismatch between active and
standby configuration.
```

というログを出力します。この状態のまま運用しますと，運用系に致命的な障害が発生したり，運用系で swap bcu コマンドを実行すると，運用系の系切替後にすべての PRU の再起動を行うため一時的に通信ができなくなります。

また，set mode コマンドで二重化モードとして動作しているときに，コンフィグレーションが運用系と待機系とで差分がある場合には，

```
E5 CONFIG 00010001 0100:000000000000 BCU swap suppressed temporarily. There is
mismatch between active and standby configuration.
```

という種別ログを出力して STATUS CODE に「01」を点灯し，EMA SUPPRESS LED を黄点灯状態にします（STATUS CODE および EMA SUPPRESS LED については，「メッセージ・ログレファレンス 1.2 障害部位の確認」を参照してください）。この場合，運用系に致命的障害が発生したり，運用系で swap bcu コマンドを実行しても，系切替実行による動作矛盾を防止するために系切替を実行しません。いったんこの種別ログが出力されると，運用系のコンフィグレーションを待機系のコンフィグレーションに合わせて設定し直しても系切替の抑止は解除できません。

運用系の系切替による通信断を回避するため，および運用系の系切替を実行可能にするには，コンフィグレーションコマンド save または copy startup-config コマンドを実行して運用系と待機系のコンフィグレーションファイルを一致させてください（実行例は「コンフィグレーションガイド　4.4 運用時の注意事項」を参照してください）。なお，copy startup-config コマンドを実行すると，待機系は自動的に再起動します。待機系が再起動したあとに上記コンフィグレーションファイル不一致の種別ログが再度出力されないことを確認してください。

5.7　セキュリティへの配慮

5.7.1　ネットワークサービス機能を停止する

次の表で示すネットワークサービス機能は，ネットワーク上の装置に対して IP 通信ができれば使用可能になりますが，使用しない機能についてはセキュリティをより向上させるため停止することをお勧めします。

表 5-16　初期導入時に使用可能なネットワークサービス機能

項番	機能	停止方法
1	リモート運用端末からの telnet プロトコルによるログイン	コンフィグレーションコマンド system telnet disable を実行する。
2	リモート運用端末からの rlogin プロトコルによるログイン	コンフィグレーションコマンド system rlogin disable を実行する。
3	リモート運用端末からの ftp プロトコルによるログイン	コンフィグレーションコマンド system ftp disable を実行する。
4	リモート運用端末からの time プロトコルによる時刻応答	コンフィグレーションコマンド system time_port disable を実行する。

5.8 冗長構成を設定する

5.8.1 コマンドによる設定

本装置では，次の表で示す装置運用に関する項目について，その運用方法を変更できます。運用方法を変更する場合は set mode コマンドを実行してください。

表 5-17 運用方法変更項目

項目	説明
基本制御モジュール運用モード	基本制御モジュール（BCU）を冗長化できます。二重化による冗長構成で運用するか，一重化で運用するかを指定してください。
電源ユニット運用モード	電源ユニットを冗長化できます。冗長化するかどうかを指定してください。冗長化した場合，立ち上げ時または電源障害などによってどちらかの電源が未接続になったときに，それを障害とみなして運用ログが採取されます。
装置起動時の優先 MC	基本制御モジュール（BCU）にある二つの MC スロット双方に MC を実装して運用する場合，装置起動時に優先的に読み込む MC のスロット位置を指定してください。

5.9 ダイアルアップ IP 接続を設定する

ダイアルアップ IP 接続でリモート運用端末を使用できます。

(1) 本装置の設定

(a) モデムの準備

「解説書 Vol.2　12.1.1 運用端末」を参照してモデムが自動着信するように設定します。

設定したモデムを本装置の AUX ポートに接続します。

(b) コンフィグレーション設定

本装置で使用する IP アドレスと，リモート運用端末で使用する IP アドレスを設定します。設定するインタフェースは aux です。

本装置で使用する IP アドレスが 200.10.10.1，リモート運用端末で使用する IP アドレスが 200.10.10.2 の場合，次の図のようにコマンドを実行します。

図 5-32　aux に関するコンフィグレーション設定例

```
(config)# line aux
[line aux]
(config)# ip 200.10.10.1/24 destination_ip_address 200.10.10.2
[line aux]
!(config)#
```

(2) リモート運用端末の設定

(a) モデムの準備

本装置にダイアルアップ IP 接続する運用端末でモデムを使用するための設定方法は，モデムのマニュアルを参照してください。

(b) 接続ソフトの設定

本装置にダイアルアップ IP 接続する運用端末にダイアルアップ IP 接続用のソフトをインストールし，次の表のように設定します。

表 5-18　ダイアルアップ IP 接続設定内容

項番	設定項目	設定内容
1	サーバーの種類	PPP
2	インターネットプロトコル (TCP/IP)	TCP ／ IP
3	IP アドレス	IP アドレスを自動的に取得する
4	DNS サーバーのアドレス	DNS サーバーのアドレスを自動的に取得する
5	認証方式	PAP ／パスワードを暗号化しない
6	電話番号	本装置に接続するモデムで使用する電話番号

(c) 認証に使用するユーザ名・パスワード

ダイアルアップ IP 接続の認証に使用するユーザ名とパスワードは，本装置のログインに使用するユーザ名とパスワードを使用します。password コマンドでパスワードを削除してあるユーザ名で認証を行う場合，入力したパスワードは無視されます。

(3) 回線接続／ログイン

(a) 回線接続

接続ソフトからダイアルします。接続に失敗する場合は「8.2　運用端末のトラブル」を参照してください。

(b) 接続確認

ダイアルアップ IP 接続を行うと IP アドレスが割り当てられます。ping コマンドなどで宛先アドレスへの通信可否を確認できます。

ダイアルアップ IP 接続が正しく行われている場合に本装置上で show sessions コマンドを使用すると，ユーザが aux ポートからログインしているように表示され，運用端末で使用している IP アドレスも表示されます。

図 5-33　show sessions コマンド実行例

(c) ログイン

リモート運用端末（リモートログイン）が使用できます。

(4) 回線切断

ダイアルアップ IP 接続は次の要因で切断されます。

- 運用端末からの切断要求
- 他ログインユーザからの killuser コマンドによるユーザ※の強制ログアウト
- 他ログインユーザからの rmuser コマンドによるユーザ※の削除
- aux ポートに関するコンフィグレーション変更／削除
- 回線障害

注※　ここでは aux ポートからログインしているユーザを指します。

6 インタフェース状態・ルーティング状態の確認

この章では，コンフィグレーションコマンドでネットワーク構成を設定したあとや運用中のトラブル発生時に行う，インタフェース状態およびルーティング状態の確認方法について説明します。

6.1 ネットワークインタフェース状態の確認

6.1.1 イーサネット回線の動作状態を確認する

イーサネット回線の動作状態確認方法は，次に示すとおりです。

(1) 状態の確認

本装置からネットワークへの回線接続を行う上で 1000BASE-X 回線を使用している場合，show interfaces コマンドを実行し，表示項目 <NIF 状態 > の表示が”active”（正常動作中），<Line 状態 > の表示が”active up”（正常動作中）であることを確認してください。表示例を次の図に示します。

図 6-1 「1000BASE-X 回線接続状態」表示例

```
> show interfaces nif 0 line 0
2003/02/23 12:00:00
NIF0: active  12-port 1000BASE-X(SFP)  retry:2
        Average:700Mbps/20Gbps  Peak:750Mbps at 08:10:30
Line0: active up  1000BASE-SX full  00:12:E2:40:0a:01
(以下省略)
>
```

なお，動作状態が正常でない場合の対応は「8.4.1　イーサネット回線の接続ができない」を参照してください。

(2) 統計情報の確認

show port statistics コマンドを実行し，本装置に実装されている全回線の送受信パケット数，送受信廃棄パケット数を確認できます。

図 6-2 「回線の動作状況確認」表示例

```
> show port statistics
2003/02/23 12:00:00
Port Counts:12
Port  Name    Status  T/R   Unicast   Multicast   Broadcast     Discard
0/ 0  GE0/0    up     Tx         0          0          0            0
                      Rx         0          0          0            0
0/ 1  GE0/1    down   Tx         0          0          0            0
                      Rx         0          0          0            0
0/ 2  GE0/2    down   Tx         0          0          0            0
                      Rx         0          0          0            0
(以下省略)
>
```

なお，本コマンド実行時に表示項目 < Discard > の表示が 0 より大きい場合はパケットが廃棄される障害が発生しています。「運用コマンドレファレンス Vol.1　show interfaces(イーサネット)」を参照して当該回線の詳細情報を取得してください。

6.1.2 リンクアグリゲーションの運用状態を確認する

リンクアグリゲーションの運用状態確認方法は，次に示すとおりです。

(1) リンクアグリゲーションの接続状態確認

show link-aggregation コマンドを実行し，表示項目 < LA Status > の表示が”Up”（データパケット送受信可能状態）であることを確認してください。また，リンクアグリゲーションに関する設定が正しいことを確認してください。

図 6-3 「リンクアグリゲーションの接続状態」表示例

```
>show link-aggregation
Date 2003/01/15 14:15:00
link-aggregation Counts:1
LA ID:1    Mode:LACP
  LA Status    :Up        Elapsed Time:10:10:39
  Multi Speed  :Off
  Max Active Port:16
  Max Detach Port:15
  Description : 6 ports are aggregated.
  MAC address: 00:12:E2:12:ff:02  VLAN ID:
  Router Interface:Switch1
  IP Address:172.16.1.249/24
  LACP Activity:Active    Periodic Timer:Short
  Actor   information: System Priority:1     MAC: 00:12:E2:12:ff:02
                       Key:101
  Partner information: System Priority:10000 MAC: 00:12:E2:f0:69:be
                       Key:100
  Port(6)        :0/1-3,10,12-13
  Up Port(2)     :0/1-2
  Down Port(4)   :0/3,10,12-13
```

(2) リンクアグリゲーションの各ポートの運用状態確認

show link-aggregation detail コマンドを実行し，リンクアグリゲーションとして集約される各ポートの表示項目 <Port> で表示されるポートがコンフィグレーションコマンド link-aggregation の aggregated-port サブコマンドで設定されている内容であることを確認してください。また，リンクアグリゲーショングループのデータパケット送受信可能状態は各ポートの運用状態の表示項目 <Status> の表示が”Up”であることを確認してください。また，<Status> の表示が”Down”で表示されるポートの障害要因は表示項目 < Reason > で確認してください。

図 6-4 「リンクアグリゲーションの各ポートの運用状態」表示例

```
>show link-aggregation detail
Date 2003/01/15 14:17:00
link-aggregation Counts:4
LA ID:1    Mode:LACP
  LA Status    :Up        Elapsed Time:10:10:39
  Multi Speed  :Off
  Max Active Port:16
  Max Detach Port:15
  Description : All 100M Full-Duplex
  MAC address: 00:12:E2:12:ff:02  VLAN ID:
  Router Interface:Switch1
  IP Address:172.16.1.249/24
  LACP Activity:Active    Periodic Timer:Short
  Actor   information: System Priority:1     MAC: 00:12:E2:12:ff:02
                       Key:101
  Partner information: System Priority:10000 MAC: 00:12:E2:f0:69:be
                       Key:100
  Port Counts:6        Up Port Counts:2
  Port:0/1   Status:Up    Reason:-
             Speed :100M  Duplex:Full
             Actor   Priority:128     Partner Priority:100
  Port:0/2   Status:Up    Reason:-
             Speed :100M  Duplex:Full
             Actor   Priority:128     Partner Priority:100
  Port:0/10  Status:Down  Reason:Duplex Half
             Speed: 100M  Duplex:Half
             Actor   Priority:128     Partner Priority:100
(以下省略)
>
```

(3) リンクアグリゲーションの統計情報の確認

show link-aggregation statistics コマンドで送受信バイト数，送受信フレーム数，送受信廃棄フレーム数を確認できます。リンクアグリゲーショングループ単位の統計情報は表示項目 <Total> で，リンクアグリ

ゲーションググループ内のポート単位の統計情報は表示項目 <Port:（NIF 番号 /Line 番号）> で確認してください。

図 6-5 「リンクアグリゲーションの統計情報」表示例

```
>show link-aggregation statistics
Date 2003/01/15 14:18:00
link-aggregation Counts:1
LA ID:1(Up)
 Total:      Octets    Tx:          12760301  Rx:              9046110
             Frames    Tx:             71483  Rx:                64377
             Discards  Tx:                96  Rx:                    9
 Port:0/1    Octets    Tx:          12745991  Rx:              9033008
             Frames    Tx:             71432  Rx:                64332
             Discards  Tx:                95  Rx:                    5
 Port:0/2    Octets    Tx:             14310  Rx:                13102
             Frames    Tx:                51  Rx:                   45
             Discards  Tx:                 1  Rx:                    4
 Port:0/3    Octets    Tx:                 0  Rx:                    0
             Frames    Tx:                 0  Rx:                    0
             Discards  Tx:                 0  Rx:                    0
(以下省略)
>
```

（4） リンクアグリゲーション LACPDU の統計情報の確認

show link-aggregation statistics lacp コマンドでリンクアグリゲーショングループ内のポート単位の送受信 LACPDU 数，送受信マーカー PDU 数，受信廃棄 PDU 数を確認できます。

図 6-6 「リンクアグリゲーション LACPDU の統計情報」表示例

```
>show link-aggregation statistics lacp
Date 2003/01/15 14:18:00
link-aggregation Counts:1
LA ID:1     Port Counts:6
  Port:1/1
    TxLACPDUs            : 50454011  RxLACPDUs   : 16507650
    TxMarkerResponsePDUs:       10  RxMarkerPDUs:        10
    RxDiscards           :        8
  Port:1/2
    TxLACPDUs            : 50454011  RxLACPDUs   : 16507650
    TxMarkerResponsePDUs:       10  RxMarkerPDUs:        10
    RxDiscards           :        8
  Port:1/3
    TxLACPDUs            :      100  RxLACPDUs   :      100
    TxMarkerResponsePDUs:       10  RxMarkerPDUs:        10
    RxDiscards           :        8
 (以下省略)
>
```

6.1.3　POS 回線の動作状態を確認する

POS 回線の動作状態確認方法は，次に示すとおりです。

（1） 状態の確認

本装置からネットワークへの回線接続を行う上で OC-192c ／ STM-64 POS 回線を使用している場合，show interfaces コマンドを実行し，表示項目 <NIF 状態 > の表示が”active”（正常動作中），<Line 状態 > の表示が”active up”（正常動作中）であることを確認してください。OC-192c ／ STM-64 POS 回線接続状態の表示例を次の図に示します。

図 6-7 「OC-192c ／ STM-64 POS 回線接続状態」表示例

```
> show interfaces nif 0 line 0
2004/02/23 12:00:00
NIF0: active  1-port OC-192c/STM-64 POS  retry:2
        Average:700Mbps/20Gbps  Peak:750Mbps at 08:10:30
Line0: active up  OC-192c/STM-64 POS(G.652-single-mode 40km)
(以下省略)
>
```

なお，動作状態が正常でない場合の対応は「8.4.8　POS でのトラブル発生時の対応」を参照してください。

（2） PPP

PPP 定義のある回線に対して show interfaces コマンドを実行し，LCP と各 NCP の状態が”up”であることを確認してください。表示例を次の図に示します。表示例は LCP，IPCP が確立しており，IPV6CP，OSINLCP，MPLSCP が未確立の状態であることを示しています。

図 6-8 「PPP 状態」表示例

```
> show interfaces nif 4 line 0
2004/04/02 12:00:00
NIF4: active  1-port OC-192c/STM-64 POS retry:2
Average:1000Mbps/20Gbps  Peak:2000Mbps at 08:10:30
Line0: active up OC-192c/STM-64 POS(G.652-single-mode 40km)
       Clock:independent CRC:32bit Scramble:on Mode:sonet
       RDI:1bit SD_BER:6 B2SD_link_down:off SF_BER:3
       Time-since-last-status-change:10:30:30
       Protocol:PPP  MRU:1500 Octets MTU:1500 Octets
       LCP:up  IPCP:up  IPV6CP:down  OSINLCP:down  MPLSCP:down
(以下省略)
>
```

（3） 統計情報の確認

show port statistics コマンドを実行し，本装置に実装されている全回線の送受信パケット数，送受信廃棄パケット数を確認できます。

図 6-9 「回線の動作状況確認」表示例

```
> show port statistics
2003/02/23 12:00:00
Port Counts:12
Port  Name    Status  T/R   Unicast   Multicast   Broadcast     Discard
0/ 0  OC0/0    up     Tx          0           0           0           0
                      Rx          0           0           0           0
0/ 1  OC0/1    down   Tx          0           0           0           0
                      Rx          0           0           0           0
0/ 2  OC0/2    down   Tx          0           0           0           0
                      Rx          0           0           0           0
(以下省略)
>
```

なお，本コマンド実行時に表示項目 < Discard > の表示が 0 より大きい場合はパケットが廃棄される障害が発生しています。「運用コマンドレファレンス Vol.1　show interfaces(POS)」を参照して当該回線の詳細情報を取得してください。

6.2　レイヤ 3 インタフェース状態の確認

6.2.1　IPv4 インタフェースの up/down を確認する

IPv4 ネットワークに接続する本装置の回線や回線内のポートに IPv4 アドレスを設定したあとに，show ip interface コマンドを実行し，IPv4 インタフェースの up/down 状態が”UP”であることを確認してください。

図 6-10 「IPv4 インタフェース状態」の表示例

```
> show ip interface summary
nagoya(0/0): UP  158.214.179.30/25
osaka(0/1): DOWN  158.214.180.30/25
fukuoka(0/2): UP  158.214.181.30/25
sapporo(0/3): DOWN  158.214.182.30/25
>
```

インタフェースが DOWN 状態の場合は，「8.5.1　通信ができない，または切断されている」を参照してください。

6.2.2　IPv6 インタフェースの up/down を確認する

IPv6 ネットワークに接続する本装置の回線や回線内のポートに IPv6 アドレスを設定したあとに，show ipv6 interface コマンドを実行し，IPv6 インタフェースの up/down 状態が”UP”であることを確認してください。

図 6-11 「IPv6 インタフェース状態」の表示例

```
> show ipv6 interface summary
tokyo: UP  3ffe::1:1/64
nagoya: UP  3ffe:1::1/64
osaka: DOWN  3ffe:2::1/64
fukuoka: UP  3ffe:3::1/64
sapporo: DOWN  3ffe:4::1/64
>
```

インタフェースが DOWN 状態の場合は，「8.8.1　通信ができない，または切断されている」を参照してください。

6.2.3　Tag-VLAN 連携通信の運用状態を確認する

本装置のイーサネットおよびギガビット・イーサネット回線で Tag-VLAN 連携通信機能を設定した場合，次の確認をしてください。

(1) 動作状態の確認

show interfaces コマンドで Tag-VLAN 連携を設定しているイーサネットおよびギガビット・イーサネット回線を指定して，表示項目 <NIF 状態 > の表示が”active”（正常動作中），<Line 状態 > の表示が”active up”（正常動作中）であることを確認してください。また，コンフィグレーションコマンド vlan で設定した vlan（Tag-VLAN 連携）回線情報が表示されていることも確認してください。

図 6-12　VLAN 回線 summary 情報表示例

```
> show interfaces nif 0 line 0
2003/02/23 12:00:00
NIF0: active  12-port 10BASE-T/100BASE-TX/1000BASE-T  retry:2
        Average:700Mbps/20Gbps  Peak:750Mbps at 08:10:30
Line0: active up  1000BASE-T full(auto)  00:12:E2:40:0a:01
        Protocol:up
(以下途中省略)
VLAN:1 Interface name: TokyoOffice1 description: Network1
        Protocol:up
        IP address:158.214.179.10  Broadcast IP address:158.214.179.255
VLAN:2 Interface name: TokyoOffice2 description: Network2
        Protocol:up
        IP address:158.214.180.12  Broadcast IP address:158.214.180.255
VLAN:untagged Interface name: TokyoOffice3 description: Network3
        Protocol:up
        IP address:158.214.185.13  Broadcast IP address:158.214.185.255
>
```

（2） 統計情報の確認

show vlans（Tag-VLAN 連携）コマンドまたは show vlan（Tag-VLAN 連携）コマンドを実行し，Tag-VLAN 連携通信が実際に運用されていること（送受信パケット数が 0 でないこと）を確認してください。

図 6-13　VLAN 回線統計情報表示例

```
> show vlans
2000/04/02 12:00:00
NIF1/LINE0:
VLAN:1 active up  Interface name: TokyoOffice1 description: Network1
Protocol:up
IP address:158.214.179.10  Broadcast IP address:158.214.179.255
<Out packets counter>                  <In packets counter>
Out packets            :       120  In packets            :       130
Out Discard packets    :         0  In Discard packets    :         0
(以下省略)
>
```

6.3　IPv4 ネットワーク状態の確認

本節では，コンフィグレーションコマンド ip で IPv4 アドレスを指定しているインタフェースの確認について説明します。

6.3.1　当該宛先アドレスとの通信可否を確認する

IPv4 ネットワークに接続している本装置のインタフェースについて，通信相手となる装置に対して通信できるかどうかを，ping コマンドを実行して確認してください。

図 6-14　ping コマンドの実行結果（通信可の場合）

```
> ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.1.51: icmp_seq=0 ttl=255 time=0.286 ms
64 bytes from 192.168.1.51: icmp_seq=1 ttl=255 time=0.271 ms
64 bytes from 192.168.1.51: icmp_seq=2 ttl=255 time=0.266 ms
^C
--- 192.168.0.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.266/0.274/0.286 ms
>
```

図 6-15　ping コマンドの実行結果（通信不可の場合）

```
> ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1): 56 data bytes
ping: sendto: エラー要因
ping: wrote 192.168.0.1 64 chars, ret=-1
ping: sendto: エラー要因
ping: wrote 192.168.0.1 64 chars, ret=-1
ping: sendto: エラー要因
ping: wrote 192.168.0.1 64 chars, ret=-1
^C
--- 192.168.0.1 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
>
```

6.3.2　当該宛先アドレスまでの経路を確認する

traceroute コマンドを実行して，IPv4 ネットワークに接続している本装置のインタフェースから通信相手となる装置までの中継装置を確認してください。

図 6-16　traceroute コマンドの実行結果

```
> traceroute 192.168.0.1 numeric
traceroute to 192.168.0.1 (192.168.0.1), 30 hops max, 40 byte packets
1  192.168.2.101  0.612 ms  0.541 ms  0.532 ms
2  192.168.1.51  0.905 ms  0.816 ms  0.807 ms
3  192.168.0.1  1.325 ms  1.236 ms  1.227 ms
>
```

6.3.3　隣接装置との ARP 解決情報を確認する

IPv4 ネットワークに接続する本装置の回線や回線内のポートに IPv4 アドレスを設定したあとに，show ip arp コマンドを実行し，本装置と隣接装置間のアドレス解決をしているか（ARP エントリ情報があるか）どうかを確認してください。アドレス解決をしていない場合は，「8.5.1　通信ができない，または切断されている」を参照してください。

6.3.4 フィルタリング機能を確認する

本装置でフィルタリング機能を使用した場合の確認内容には次のものがあります。

(1) 運用中の確認

(a) 統計情報の確認

show filter-flow コマンドを実行してフローフィルタ統計情報を表示し，廃棄されているパケット数を確認してください。廃棄パケット数が多い場合，本来はパケット廃棄をしてはいけない通信部位かもしれません。現在のネットワークの運用状況を確認してください。

図 6-17 フィルタリングによるパケット廃棄数表示

```
> show filter-flow interface tokyo1 detail
<Filter IP List No.>:    1
      Using Interface:tokyo1/in
      ip source: 170.10.11.21 - 170.10.11.30
      ip destination: any
      protocol:ip
      forward packets                                  :                 461
<Filter IP List No.>:    2
      Using Interface:tokyo1/in
      ip source: any
      ip destination: any
      protocol:ip
      drop packets                                     :               50121
<Filter IP List No.>:    1
      Using Interface:tokyo1/out
      source ip :170.10.12.1 - 170.10.12.254
      ip destination: any
      protocol:ip
      forward packets                                  :                   3
(以下省略)
>
```

6.3.5 ポリシールーティング機能を確認する

本装置でポリシールーティング機能を使用した場合の確認内容には次のものがあります。

(1) コンフィグレーション設定後の確認

(a) 入力先インタフェースの設定確認

show ip local policy コマンドを実行し，入力先インタフェースの現在のポリシールーティング条件がコンフィグレーションコマンド flow filter で設定されている内容であることを確認してください。

図 6-18　入力先インタフェースの動作状態表示

```
> show ip local policy interface tokyo
<Interface Name>: tokyo <Filter List No.> 1
        forward packets
        protocol                   : ip
        ip_source                  : 200.1.4.0 - 200.1.4.255
        ip_destination             : 200.1.7.0 - 200.1.8.255
        current policy route
          Policy Group Name          route1
          Output Interface           tokyo3
          Next Hop IP address        200.1.10.1
<Interface Name>: tokyo <Filter List No.> 2
        forward packets
        protocol                   : ip
        ip_source                  : 200.1.5.0 - 200.1.5.255
        ip_destination             : 200.1.19.0 - 200.1.20.255
        current policy route
          Policy Group Name          route2
          Output Interface           yokohama
          Next Hop IP address        200.1.50.2
(以下省略)
>
```

(2) 運用中の確認

(a) 出力先インタフェースの状態確認

show ip cache policy コマンドを実行し，出力先インタフェースの動作状態が UP であることを確認してください。

図 6-19　出力先インタフェースの動作状態表示

```
> show ip cache policy route1
<Policy Group Name>:     route1
       priority  Interface Name  status   Nexthop
   *>      1     tokyo1            Up     200. 1. 1.  2
           2     tokyo1            Up     200. 1. 2.  2
           3     tokyo2            Down   200. 1. 8.  3
           4     tokyo3            Down   200. 1. 10. 1    default
>
```

6.3.6 Null インタフェースを確認する

本装置で Null インタフェースの機能を使用した場合の確認内容には次のものがあります。

(1) コンフィグレーション設定後の確認

(a) 経路情報の確認

show ip route コマンドを実行し，コンフィグレーションコマンド static で定義した経路情報の設定内容が正しく反映されているかどうかを確認してください。

図 6-20　Null インタフェース経路情報表示

```
> show ip route static
Total: 3 routes
Destination          Next Hop         Interface     Metric  Protocol  Age
172.16.250/24        192.168.11.101   rmEthernet    0/0     Static     1h  8m
172.16.251.89/32     ----             null          0/0     Static     1m  9s
(以下省略)
>
```

(2) 運用中の確認

(a) パケット廃棄数の確認

show ip interface コマンドを実行し，Null インタフェースでパケットが廃棄されているかどうかを確認し

てください。

図 6-21　Null インタフェースパケット廃棄数表示例

```
> show ip interface delete-packets null-interface
Interface Name:null
Discard Packets(IPv4) :92(pkts)
>
```

6.3.7　ロードバランスで使用する選択パスを確認する

(1)　コンフィグレーション設定後の確認

(a)　経路情報の確認

show ip route コマンドを実行し，定義したマルチパス経路の設定内容が正しく反映されているかどうかを確認してください。

図 6-22　マルチパスの経路情報表示

```
> show ip route
Total: 4 routes
Destination         Next Hop         Interface       Metric   Protocol  Age
172.16.10/24        172.16.10.1      LAN01           0/0      Direct    29s
172.16.10.1/32      172.16.10.1      LAN01           0/0      Direct     1h 12m
172.16.20.2/24      192.168.10.1     LAN10           0/0      Static     1h 10m
                    192.168.20.1     LAN20           -        -         -
                    192.168.30.1     LAN30           -        -         -
                    192.168.40.1     LAN40           -        -         -
172.16.100.2/24     172.16.10.2      LAN01           2/0      RIP       29s
>
```

(b)　当該宛先アドレスとの通信可否を確認する

ロードバランスで使用する本装置のインタフェースについて，通信相手となる装置に対して通信できるかどうかを，ping <IPv4 Address> specific-route source <Source Address> コマンドを実行して確認してください。ping コマンドの <Source Address> にはロードバランスで使用するインタフェースの本装置の自 IPv4 アドレスを指定してください。

6.3.8　マルチホーム接続を確認する

(1)　コンフィグレーション設定後の確認

(a)　経路情報の確認

show ip interface コマンドを実行し，該当インタフェースにコンフィグレーションコマンド ip-address でマルチホーム接続として定義した IPv4 アドレスが正しく反映されているかどうかを確認してください。

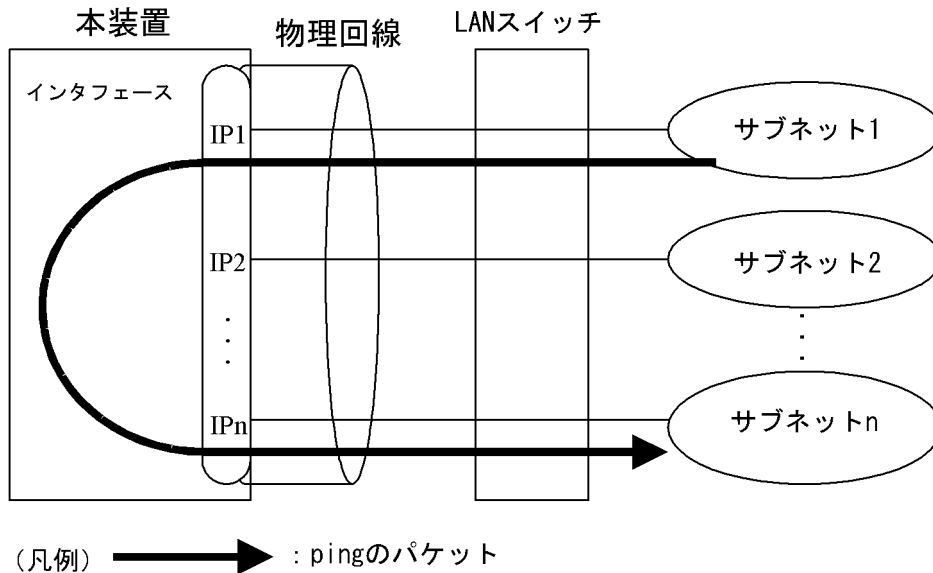
図 6-23　マルチホーム接続時の IPv4 アドレス表示

```
> show ip interface
tokyo1:  flags=80e3<UP,BROADCAST,NOTRAILERS,RUNNING,NOARP,MULTICAST>
         mtu 1500
         inet 172.16.10.1/24 broadcast 172.16.10.255
         inet 172.16.20.1/24 broadcast 172.16.20.255
         inet 172.16.30.1/24 broadcast 172.16.30.255
         NIF0/Line0: UP media 100BASE-TX full(auto) 00:12:E2:d0:97:d8
         Time-since-last-status-change: 00:00:30
         Last down at: 08/21 16:21:01
>
```

(b)　当該宛先アドレスとの通信可否を確認する

本装置からマルチホーム接続の通信相手となる装置に対して通信できるかどうかを，ping コマンドを実行

して確認してください。さらに，本装置とマルチホーム接続であり，同じインタフェースを使用している装置同士で通信できるかどうかを，ping コマンドを実行して確認してください。

図 6-24　マルチホーム接続を確認する ping の流れ

6.3.9　DHCP ／ BOOTP リレーエージェント機能を確認する

本装置で DHCP ／ BOOTP リレーエージェント機能を設定した場合の確認内容には次のものがあります。

(1)　コンフィグレーション設定後の確認

(a)　DHCP ／ BOOTP サーバへの通信確認

本装置からコンフィグレーションコマンド relay-list で設定した DHCP ／ BOOTP サーバまたは DHCP ／ BOOTP サーバが存在しているネットワークまでの，中継可能なルータの IP アドレスに対して通信ができるかどうかを，ping コマンドを実行して確認してください。

(b)　リレーエージェントアドレスの確認

show dhcp giaddr コマンドを実行し，出力された IP アドレスがコンフィグレーションコマンド relay-interface で設定したインタフェースの IP アドレスであることを確認してください。

図 6-25　DHCP ／ BOOTP giaddr 表示

```
> show dhcp giaddr interface Department1
DHCP GIADDR < Department1> : 130.3.3.1
>
```

show dhcp giaddr コマンドを実行し，出力された IP アドレスが「DHCP ／ BOOTP クライアントが接続されている本装置設定 IP アドレス」と一致していることを確認してください。特に，クライアント接続インタフェースにマルチホームの設定がある場合，relay_agent_address パラメータを省略するとそのインタフェースに最後に定義した IP アドレスをリレーエージェントアドレスとして設定しているので注意してください。次に構成例および実行例を示します。

[構成例]

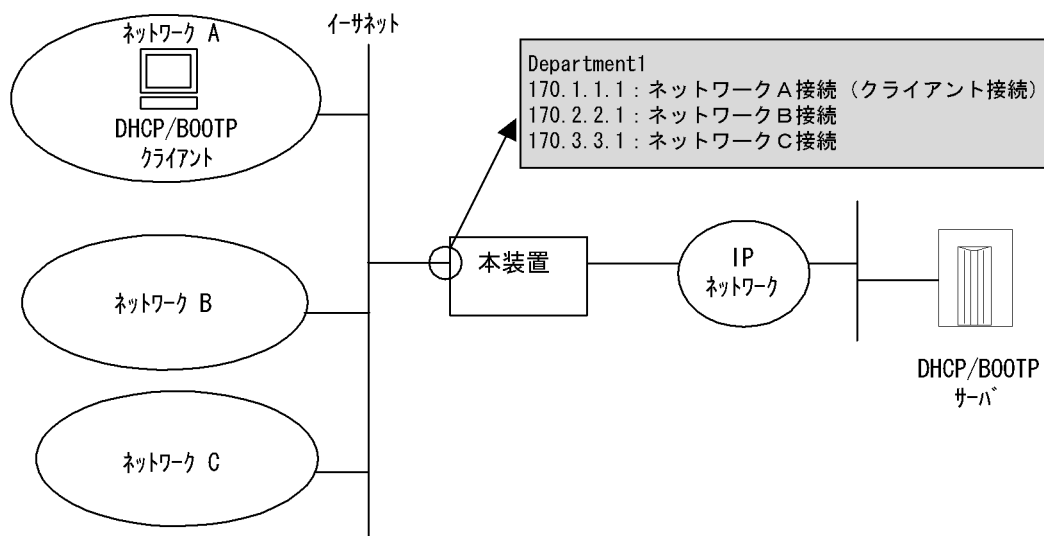



図 6-26　DHCP ／ BOOTP giaddr 表示

```
> show dhcp giaddr interface Department1
DHCP GIADDR < Department1> : 170.1.1.1
>
```

なお，出力された IP アドレスが，DHCP ／ BOOTP クライアントが接続されている本装置 IP アドレスと一致していない場合の対応は，「8.5.2　DHCP 機能で IP アドレスが割り振られない」を参照してください。

6.3.10　DHCP サーバ機能を確認する

本装置で DHCP サーバ機能を設定した場合の確認内容には次のものがあります。

(1)　コンフィグレーション設定時の確認

(a)　DHCP リレーエージェント装置との通信確認

DHCP リレーエージェントを経由して DHCP クライアントに IP アドレスを割り当てる場合，DHCP リレーエージェント装置に対して通信できるかどうかを，ping コマンドを実行して確認してください。

(b)　割り当て IP アドレスプール数の確認

本装置で接続できるクライアントの台数（IP アドレスプールの数）は 8192 台です。show ip dhcp server statistics コマンドを実行し，コンフィグレーションコマンド dhcp subnet や dhcp host で設定した，クライアントに割り当てる IP アドレスの数を確認してください。

図 6-27　割り当て IP アドレスプール数表示例

```
> show ip dhcp server statistics
   < DHCP Server use statistics >
     address pools          :10
     automatic bindings     :0
(以下省略)
>
```

(2) 運用中の確認

(a) 割り当て済み IP アドレス数の確認

実際に DHCP クライアントへ割り当てられた IP アドレスについては，show ip dhcp binding コマンドを実行して確認してください。リースを満了していない IP アドレスが表示されます。

図 6-28 割り当て済み IP アドレス数表示例

```
> show ip dhcp binding
<IP address>     <MAC address>        <Lease expiration>   <Type>
192.168.200.9    00:12:E2:48:e9:2d    01/12/06 19:59:40    Automatic
192.168.200.99   00:12:E2:92:f7:b9                         Manual
>
```

6.3.11 DNS リレー機能を確認する

本装置で DNS リレー機能を使用した場合の確認内容には次のものがあります。

(1) コンフィグレーション設定後の確認

(a) ネームサーバの設定確認

show dns-relay コマンドを実行し，コンフィグレーションコマンド dns-resolver で設定したネームサーバの IP アドレスが表示されることを確認してください。

図 6-29 ネームサーバ IP アドレス表示例

```
> show dns-relay
Primary   NameServer: 192.168.253.177
Secondary NameServer: 192.168.253.178
Thirdary  NameServer: -
(以下省略)
>
```

```
> show interfaces OsakaISP2
2002/04/05 10:56:30
NIF2: active  4-port 10BASE-T/100BASE-TX  retry:0
       Average:0/800Mbps  Peak:150Mbps at 13:53:03
Line0: active up  100BASE -TX full(auto)  00:12:E2:a8:c5:1c
        Average out:20Mbps  Average in:10Mbps
PPPoE:OsakaISP2 connected  Session ID:e714  retry:0
       Connected time 02/13 00:00:00  Connecting time 1234:56:30
        Auto connection timer(past/setting): ---/10(sec)
       Service Name:OsakaISPservice1
        AC Name:OsakaISP01server
        Destination MAC address 00:12:E2:a8:fe:2c
        Source IP address:192.168.100.1  Destination IP address:192.168.35.2
        Primary DNS server IP address: 128.10.10.1
        Secondary DNS server IP address: 128.10.10.10
                      ~
        CHAP Challenge timeout  :
>
```

両方またはどちらかのアドレスが取得されていること

(b) ネームサーバへの通信確認

コンフィグレーションコマンド dns-resolver で設定した IP アドレスについて，本装置と疎通できることを，ping コマンドを実行して確認してください。

(2) 運用中の確認

(a) 動作状態確認

show dns-relay コマンドを実行し，DNS リレーの動作状態を確認してください。

なお，確認内容の詳細は「8.5.4　DNS リレー通信でドメイン解決ができない」を参照してください。

6.4 IPv4 ユニキャストルーティング情報の確認

6.4.1 宛先アドレスへの経路を確認する

本装置で IPv4 ユニキャストルーティング情報を設定した場合は，show ip route コマンドを実行して宛先アドレスへの経路が存在していることを確認してください。存在しない場合は，「6.4.2 RIP のゲートウェイ情報を確認する」～「6.4.4 BGP4 のピアリング情報を確認する【OP-BGP】」について確認してください。

図 6-30 show ip route コマンドの実行結果

```
> show ip route
Total: 10 routes
Destination          Next Hop          Interface   Metric   Protocol    Age
127/8                127.0.0.1         -           0/0      Direct      300
127.0.0.1/32         127.0.0.1         -           0/0      Direct      300
          :
192.168.2/24         192.168.2.101     PAIR1       3/0      RIP         100
          :
>
```

宛先アドレスへの経路が存在するかどうかを確認してください

6.4.2 RIP のゲートウェイ情報を確認する

本装置の IPv4 ユニキャストルーティング情報で RIP 機能を設定した場合は，show ip rip gateway を実行して，次のことを確認してください。

- Gateway Address 内に当該経路を広告すべき隣接ルータが存在するか確認してください。存在しない場合，隣接ルータから RIP パケットを受信していません。隣接ルータまたは隣接ルータと接続されたインタフェースを調査してください。
- Age が 30 秒以内になっていることを確認してください。30 秒以上になっている場合，隣接ルータから周期的に RIP パケットが到達していません。隣接ルータまたは隣接ルータと接続されたインタフェースを調査してください。
- Flags に Format，AuthFail が表示されていないか確認してください。Format，AuthFail が表示されている場合，隣接ルータから不正な RIP パケットを受信しています。隣接ルータを調査してください。
- Flags に Reject が表示されていないか確認してください。Reject が表示されている場合，当該ルータからの RIP パケットの受信が拒否状態となっています。コンフィグレーションの rip コマンド（interface 指定）で当該インタフェースに ripin パラメータを指定してください。
- Flags に ImportRestrict が表示されていないか確認してください。ImportRestrict が表示されている場合，インポートフィルタにより当該経路の取り込みがフィルタリングされている可能性があります。コンフィグレーションのインポートフィルタを調査してください。
- その他の場合，隣接ルータが当該経路を広告していない可能性があります。隣接ルータを調査してください。

図 6-31　show ip rip gateway コマンドの実行結果

```
> show ip rip gateway
Gateway Address Age        Flags
192.168.50.185   1s      <Accept>
192.168.60.30   14s      <Accept>
192.168.70.30    9s      <Accept>
     :
>
```

6.4.3　OSPF のインタフェース情報を確認する

本装置の IPv4 ユニキャストルーティング情報で OSPF 機能を設定した場合は，show ip ospf interface <IP Address> または show ip ospf interface detail を実行して，次のことを確認してください。

- Neighbor List 内に当該経路を広告すべき隣接ルータが存在するか確認してください。存在しない場合，隣接ルータから Hello パケットを受信していません。隣接ルータまたは隣接ルータと接続されたインタフェースを調査してください。
- インタフェースの状態が DR または P to P の場合，Neighbor List 内の全隣接ルータ状態が Full となっていることを確認してください。
    - Full でない場合，隣接ルータとの隣接関係が確立していません。隣接ルータを調査してください。
- インタフェースの状態が BackupDR または DR Other の場合，Neighbor List 内より DR となる隣接ルータが存在するか確認してください。
    - DR が存在し，DR の隣接ルータ状態が Full でない場合，DR との隣接関係が確立していません。隣接ルータを調査してください。
    - DR が存在しない場合は，自装置および隣接ルータの priority が設定されていない可能性があります。自装置および隣接ルータの priority を確認してください。

図 6-32　show ip ospf interface コマンドの実行結果

```
> show ip ospf interface 192.168.50.1
Domain: 1
Index: 2, Name: Office1, Address: 192.168.50.1, State: BackupDR
Auth Type: Simple
MTU: 1436, DDinPacket: 70, LSRinPacket: 117, ACKinPacket: 70
Router ID: 172.168.50.1, Network Type: Broadcast
Area: 0.0.0.0, DR: 192.168.50.2, Backup DR: 192.168.50.1
Priority: 1, Cost: 1
Intervals:
Hello: 10s, Dead Router: 40s, Retransmission: 5s, Delay: 1s, Poll: 120s

Neighbor List (1):
Address         State      RouterID     Priority DR              Backup DR
192.168.50.2    Full       192.168.50.2    1     192.168.50.2   192.168.50.1
    :
>
```

6.4.4　BGP4 のピアリング情報を確認する【OP-BGP】

本装置の IPv4 ユニキャストルーティング情報で BGP4 機能を設定した場合は，show ip bgp neighbors を実行して，次のことを確認してください。

- BGP Status が Established 状態となっていることを確認してください。Established 状態以外の場合，相手 BGP4 スピーカとのピアリングが確立していません。相手 BGP4 スピーカとの通信が可能か ping コマンドなどで調査してください。不可能な場合，自装置と相手 BGP4 スピーカ間のインタフェースまたはルータが障害となっている可能性があります。traceroute コマンドなどで障害部位を特定し，障害部位を調査してください。可能な場合，相手 BGP4 スピーカを調査してください。

● BGP Status が Established 状態の場合，相手 BGP4 スピーカが当該経路を広告していない可能性があります。相手 BGP4 スピーカを調査してください（相手 BGP4 スピーカが当該経路情報を広告しているかどうかは，show ip bgp route コマンドで確認できます）。

図 6-33　show ip bgp neighbors コマンドの実行結果

```
> show ip bgp neighbors 192.168.50.2
BGP Peer: 192.168.50.2, Remote AS: 1810
Remote Router ID: 192.168.22.200, Policy Group: 1
    BGP Status: Established         HoldTime: 90
    Established Transitions: 1      Established Time: 16:25:34
    BGP Version: 4                  Type: External
    Local Address: 192.168.50.1     Local AS: 2735
    Local Router ID: 192.168.22.100
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 18:42:20  Last Keep Alive Receive: 18:42:20
    Graceful Restart: Both
      Restart Status : Receiving   2004/07/08 17:01:23
      Receive Status : Finished    2004/07/07 10:11:12
       Stale Routes Retain Time: 30
    NLRI of End-of-RIB Marker: Advertised and Received
    BGP Messages UpdateIn UpdateOut TotalIn TotalOut
                       12        14      36       42
    BGP Capability negotiation: <IPv4-Uni, GracefulRestart >
      Send   : <IPv4-Uni, GracefulRestart(RestartTime:120s)>
      Receive: <IPv4-Uni, GracefulRestart(RestartTime:300s, IPv4-uni)>
    Authentication : TCP MD5
    No fast fallover : configured
>
```

6.4.5　IS-IS の隣接情報を確認する【OP-ISIS】

本装置の IPv4 ユニキャストルーティング情報で IS-IS 機能を設定した場合は，show isis adjacency を実行し，次のことを確認してください。

● Adjacencys 内に当該経路を広告すべき隣接ルータが存在するか確認してください。存在しない場合，隣接ルータから Hello パケットを受信していません。隣接ルータまたは隣接ルータと接続されたインタフェースを調査してください。

● State が Up 状態となっていることを確認してください。Up 状態以外の場合，隣接ルータが本装置を認識していません。隣接ルータを調査してください。

● State が Up 状態の場合，隣接ルータが当該経路を広告していない可能性があります。隣接ルータを調査してください（隣接ルータが当該経路情報を広告しているかどうかは，show isis database コマンドで確認できます）。

図 6-34　show isis adjacency コマンドの実行結果

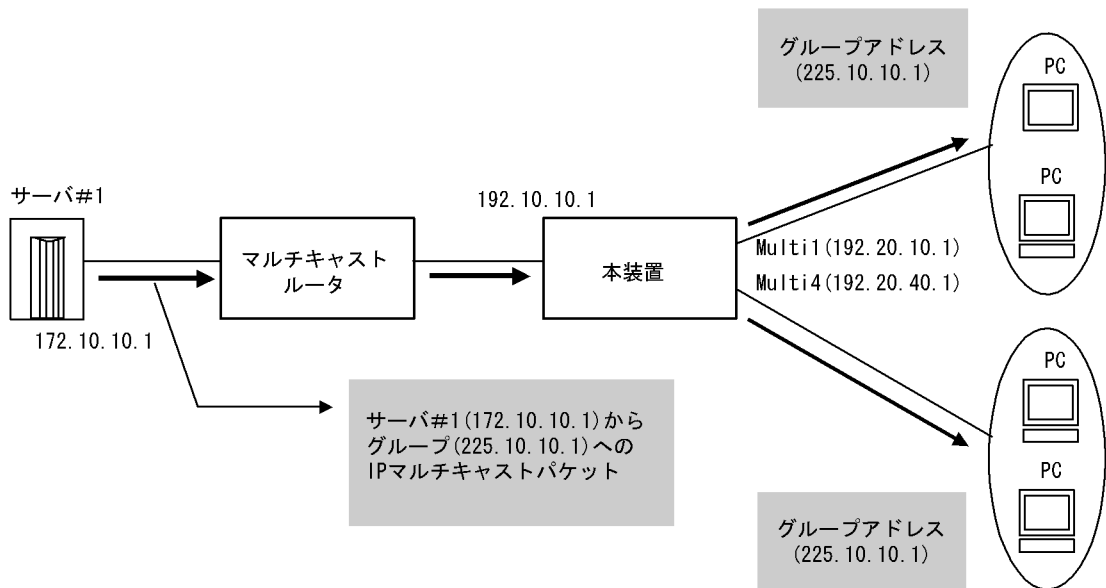
```
> show isis adjacency detail
Level-1 adjacencies
Interface: Office1, Interface Type: Broadcast
    System ID: 0000.87c0.3655, Type: IS, State: Up
    Speaks: IP
    Area: 49
    Circuit ID: 0x04, SNPA: 00:12:E2.c0.36.55
    Priority : 64, Hold Timer: 9s, Established Time: 2003/07/01 15:30:00
    Interface Address: 192.168.7.2
>
```

6.5　IPv4 マルチキャストルーティング情報の確認【OP-MLT】

6.5.1　宛先グループアドレスへの経路を確認する

本装置で IPv4 マルチキャストルーティング情報の設定を行った場合は，show ip mcache コマンドを実行して宛先アドレスへの経路が存在していることを確認してください。存在しない場合，および downstream が正しくない場合は，「6.5.2　PIM-DM，PIM-SM 情報を確認する」～「6.5.4　IGMP 情報を確認する」について確認してください。

図 6-35　show ip mcache コマンドの実行結果

```
> show ip mcache
Total: 1 routes
Group Address      Source Address     Uptime    Expires   Upstream
225.10.10.1        172.10.10.1        01:00     02:00     192.10.10.1
     downstream:
         Multi1(192.20.10.1)
         Multi4(192.20.40.1)
>
```

6.5.2　PIM-DM，PIM-SM 情報を確認する

本装置の IPv4 マルチキャストルーティング情報で，PIM-DM 機能または PIM-SM 機能を設定した場合の確認内容には次のものがあります。

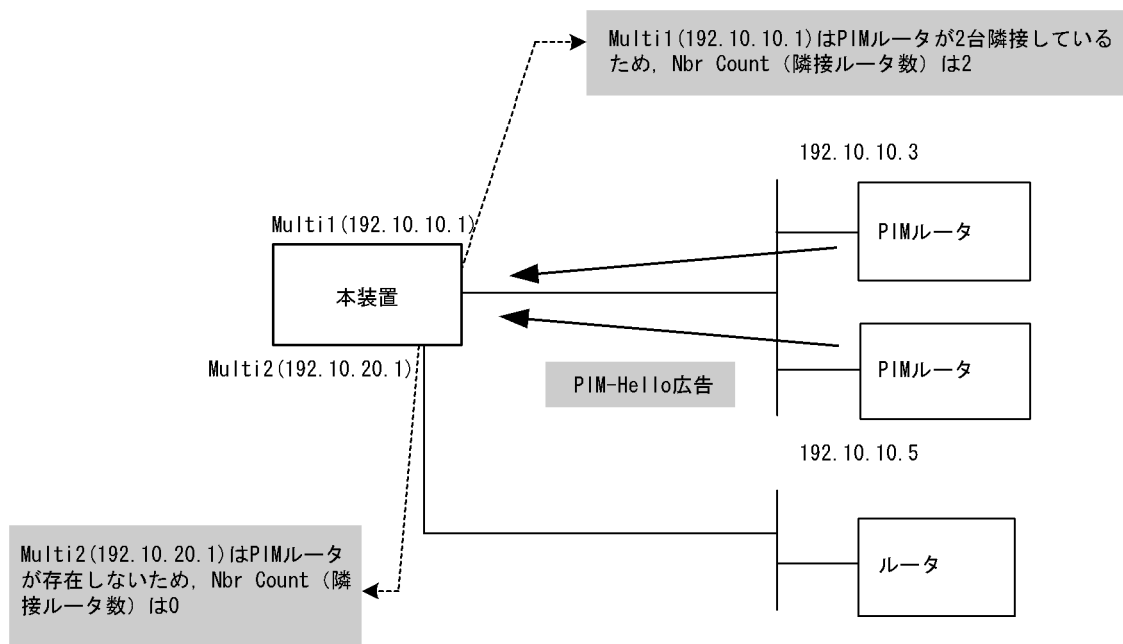
(1) インタフェース情報

show ip pim interface を実行して，次のことを確認してください。

- Address 内のインタフェースを確認してください。存在しない場合，そのインタフェースで PIM-DM および PIM-SM は動作していません。コンフィグレーションで当該インタフェースで PIM が enable になっているか確認してください。また，そのインタフェースに障害が発生していないか確認してください。

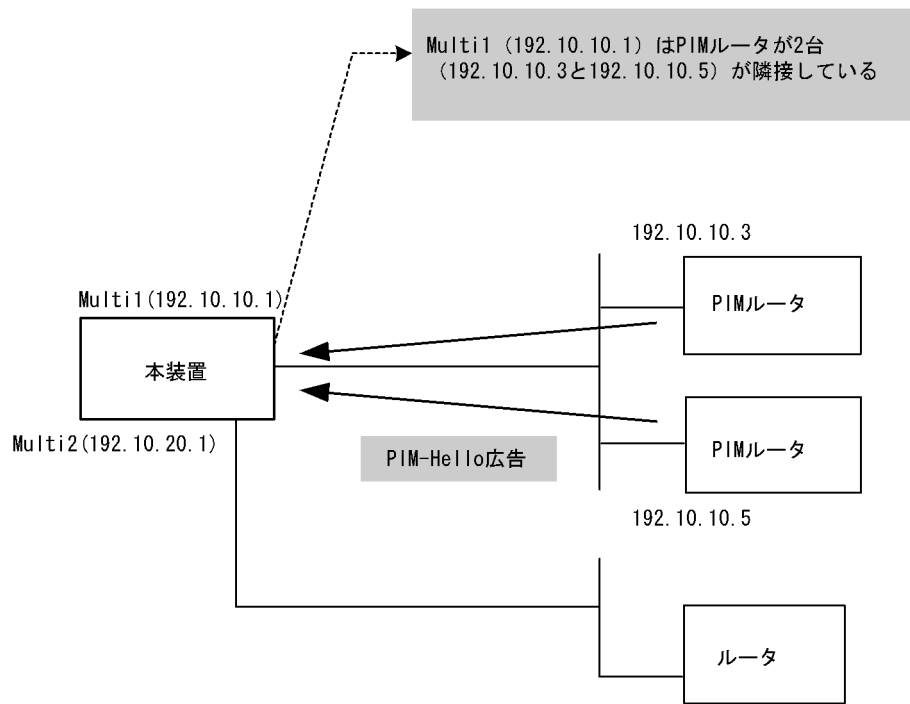
● 該当インタフェースの Nbr Count（PIM 隣接ルータ数）を確認してください。0 の場合は隣接ルータが存在しないか，隣接ルータが PIM-Hello を広告していない可能性があります。隣接ルータを調査してください。

図 6-36　show ip pim interface コマンドの実行結果

```
[PIM-DMの場合の表示]

> show ip pim interface
Address         Interface     Component   Vif   Nbr      Query    JP       C-RP       DR
                                                Count    Intvl    Intvl
192.10.10.1     Multi1        PIM-DM      1     2        30       -        -          -
192.10.20.1     Multi2        PIM-DM      2     0        30       -        -          -
>

[PIM-SMの場合の表示]

> show ip pim interface
Address             Interface     Component   Vif    Nbr       Hello    DR
                                                     Count     Intvl    Address
192.10.10.1         Multi1        PIM-SM      1      2         30       192.10.10.5
192.10.20.1         Multi2        PIM-SM      2      0         30       192.10.20.1
>
```

(2) 隣接情報

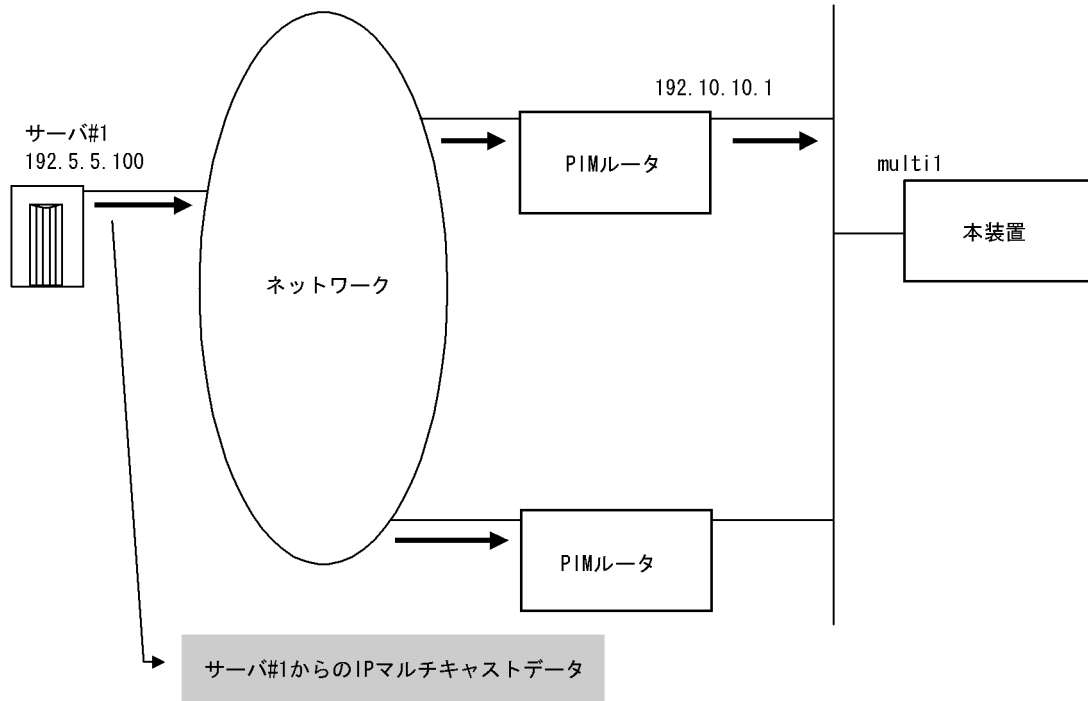
show ip pim neighbor を実行し，当該インタフェースの NeighborAddress 内の IP アドレスで隣接相手を確認してください。ある特定の隣接が存在しない場合，隣接ルータが PIM-Hello を広告していない可能性があります。隣接ルータを調査してください。

図 6-37　show ip pim neighbor コマンドの実行結果

```
> show ip pim neighbor
Address          Interface        NeighborAddress   Uptime    Expires
192.10.10.1      Multi1           192.10.10.3       00:05     01:40
                                  192.10.10.5       00:10     01:35
>
```


(3) 送信元ルート情報

show ip rpf コマンドを実行し，送信元のルート情報を確認してください。

図 6-38 show ip rpf コマンドの実行結果

（4） PIM-SM BSR 情報

show ip pim bsr を実行し，BSR アドレスが表示されていることを確認してください。”----” 表示の場合，BSR が Bootstrap メッセージを広告していないか，BSR が存在していない可能性があります。BSR を調査してください。なお，PIM-SSM では BSR は使用しないので注意してください。

図 6-39 show ip pim bsr コマンドの実行結果

```
> show ip pim bsr
Status: Not Candidate Bootstrap Router
BSR Address:192.10.10.10
    Priority:100,Hash Mask length:30
    Uptime:03:00
    Bootstrap Timeout:130 seconds
>
```

（5） PIM-SM ランデブーポイント情報

show ip pim rendezvous-point mapping を実行し，該当の IPv4 マルチキャストグループアドレスに対する C-RP Address が表示されていることを確認してください。表示のない場合，BSR が Bootstrap メッセージを広告していないか，ランデブーポイントまたは BSR が存在していない可能性があります。ランデブーポイントおよび BSR を調査してください。なお，PIM-SSM ではランデブーポイントは使用しないので注意してください。

図 6-40　show ip pim rendezvous-point mapping コマンドの実行結果

```
> show ip pim rendezvous-point mapping
Status: Not Candidate Rendezvous Point
Total: 2 routes, 2 group, 1 RPs
Group/masklen         C-RP Address        pri   Uptime  Expires
224.100.100.0/24      192.1.1.1           100   02:00   02:30
224.100.200.0/24      192.1.1.1           100   02:00   02:30
>
```

(6) PIM-SM ルーティング情報

show ip mroute コマンドを実行し，当該宛先アドレスへの経路が存在するかどうかを確認してください。(S,G) エントリが存在しない場合は，(*,G) エントリが存在しているかを確認してください。(*,G) が存在しない場合，および in-coming.downstream が正しくない場合は隣接ルータを調査してください。なお，PIM-SSM では (*,G) は使用しません (存在しません)。

図 6-41　PIM-SM マルチキャストルート情報の表示

```
> show ip mroute
Total: 5 routes, 3 groups, 2 RPs
(S,G) 2 routes -------------------------------------------------------------
Group Address      Source Address   Protocol Flags  Uptime  Expires  Assert
224.100.100.10     192.1.1.1        SM       F      02:00   02:30    01:00
    in-coming : Multi1(192.1.1.3)                 upstream: Direct, Reg-Sup: 60s
    downstream: Multi2(192.1.2.3)                 uptime 02:30, expires 00:40
224.100.100.20     192.1.1.1        SM       F      02:00   02:30    01:00
    in-coming : Multi1(192.1.1.3)                 upstream: Direct
    downstream: Localhost(127.0.0.1) <Register to 192.1.5.1>
224.100.100.30     192.1.4.1        SM       F      02:00   02:30    01:00
    in-coming : Multi1(192.1.1.3)                 upstream: 192.1.1.5
    downstream: Multi2(192.1.2.3)                 uptime 02:30, expires 00:40

(*,G) 2 routes -------------------------------------------------------------
Group Address      RP Address       Protocol Flags  Uptime  Expires  Assert
225.100.100.10     192.1.5.1        SM       R      02:00   02:30    01:00
    in-coming : Localhost(127.0.0.1)              upstream: This System
    downstream: Multi2(192.1.2.3)                 uptime 02:30, expires 00:40
225.100.100.10     192.1.5.1        SM       R      02:00   02:30    01:00
    in-coming : Multi1(192.1.1.3)                 upstream: 192.1.1.2
    downstream: Multi3(192.1.3.3)                 uptime 02:30, expires 00:40
>
```

6.5.3　DVMRP 情報を確認する

本装置の IPv4 マルチキャストルーティング情報で DVMRP 機能を設定した場合の確認内容には次のものがあります。

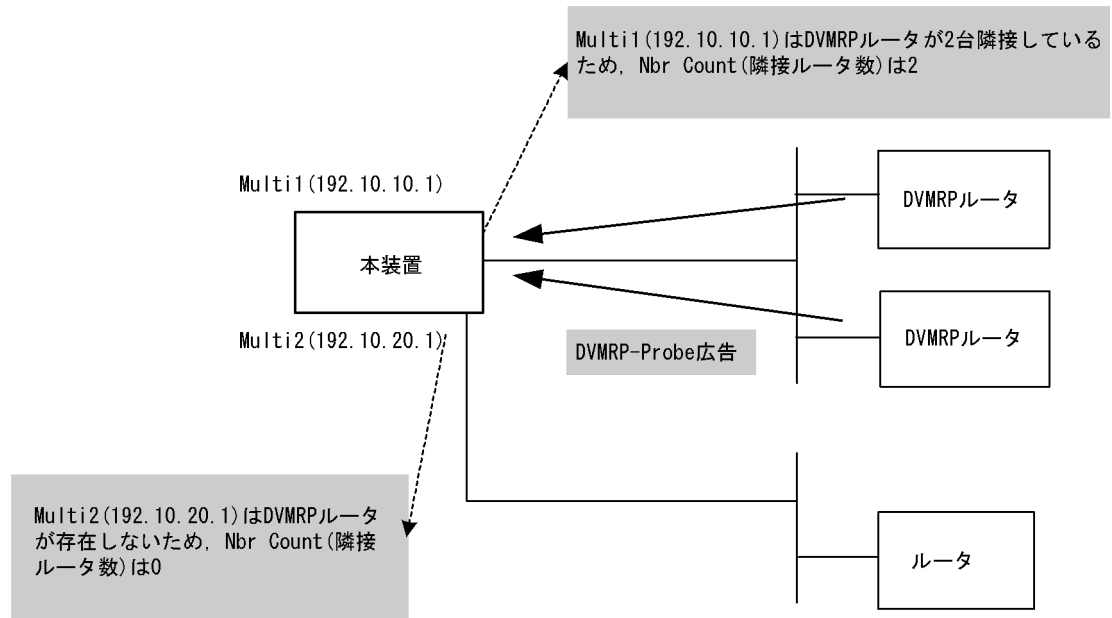
(1) インタフェース情報

show ip dvmrp interface を実行し，次のことを確認してください。

● Address 内のインタフェースを確認してください。存在しない場合，そのインタフェースで DVMRP は動作していません。コンフィグレーションで当該インタフェースで DVMRP が enable になっているか確認してください。また，そのインタフェースに障害が発生していないか確認してください。

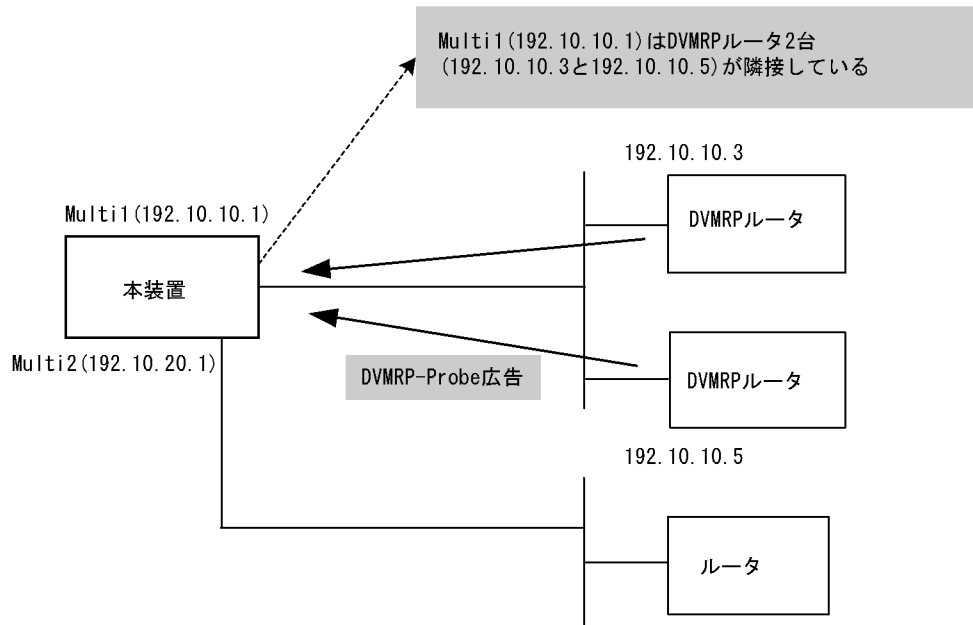
● 該当インタフェースの Nbr Count (DVMRP 隣接ルータ数) を確認してください。0 の場合は隣接ルータが存在しないか，隣接ルータが DVMRP-Probe を広告していない可能性があります。隣接ルータを調査してください。

図 6-42　show ip dvmrp interface コマンドの実行結果

```
> show ip dvmrp interface
Address          Interface   Component  Vif    Nbr      #Bad     #Bad      Kind
                                               Count    Pkts     Pkts
192.10.10.1      Multi1      DVMRP       1       2       0         0        -
192.10.20.1      Multi2      DVMRP       2       0       0         0        -
>
```


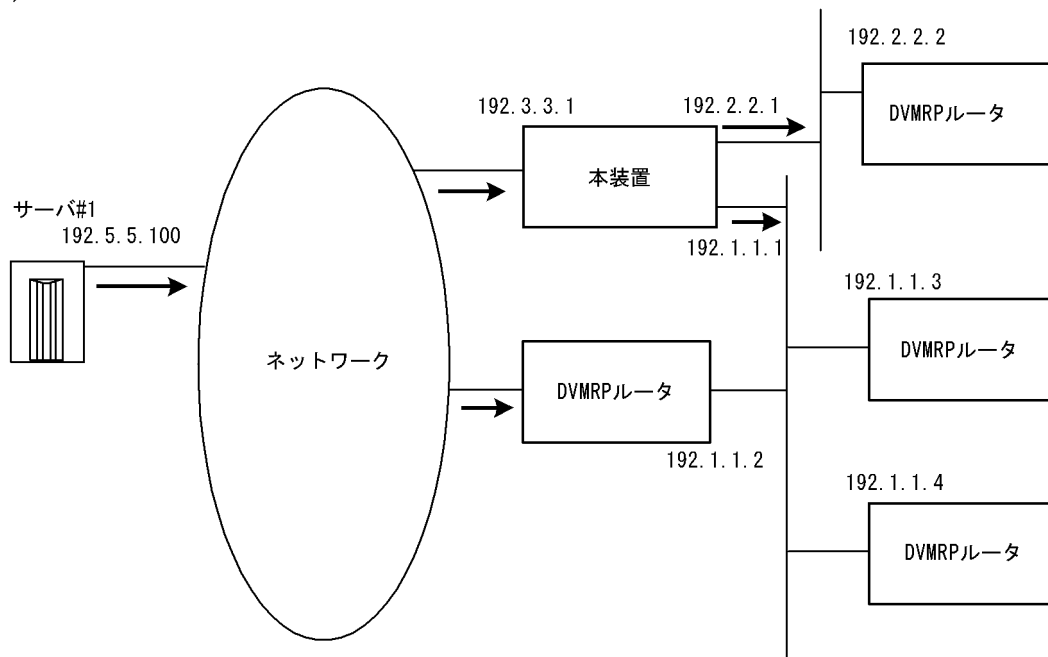
(2) 隣接情報

show ip dvmrp neighbor を実行し，当該インタフェースの NeighborAddress 内の IP アドレスで隣接相手を確認してください。ある特定の隣接が存在しない場合，隣接ルータが DVMRP-Probe を広告していない可能性があります。隣接ルータを調査してください。

図 6-43　show ip dvmrp neighbor コマンドの実行結果

(3) 送信元ルート情報

show ip dvmrp route を実行し，送信元のルート情報を確認してください。

図 6-44　show ip dvmrp route コマンドの実行結果

```
> show ip dvmrp route 192.5.5.100
RPF Information for ? (192.5.5.100): lif multi1(192.3.3.1)
DownstreamIface    Forwarder             Depnbrs
192.1.1.1          192.1.1.1             2
                                         DepNbr   192.1.1.3
                                         DepNbr   192.1.1.4
192.2.2.1          192.2.2.1             1
                                         DepNbr   192.2.2.2
>
```

6.5.4　IGMP 情報を確認する

本装置の IPv4 マルチキャストルーティング情報で IGMP 機能を設定した場合の確認内容には次のものがあります。

（1）インタフェース情報

show ip igmp interface を実行し，次のことを確認してください。

- Address 内のインタフェースを確認してください。存在しない場合，そのインタフェースで IGMP は動作していません。PIM が動作している場合，コンフィグレーションの当該インタフェースで PIM が enable，DVMRP が動作している場合，コンフィグレーションの当該インタフェースで IGMP が enable かつ DVMRP が enable になっているか確認してください。また，そのインタフェースに障害が発生していないか確認してください。
- 該当インタフェースの Group Count（加入グループ数）を確認してください。0 の場合は加入グループが存在しないかグループ加入ホストが IGMP-Report を広告していない可能性があります。ホストを調査してください。
- Version 欄に表示されているバージョンが当該インタフェースで使用しているホストと接続可能であるか確認してください。

● Notice 欄にコードが表示される場合は IGMP パケットが廃棄されています。コードから廃棄理由を調査してください。

図 6-45　show ip igmp interface コマンドの実行結果

```
> show ip igmp interface
Total: 5 Interfaces
Address        Interface     Querier         Expires  Version  Group Count  Notice
192.10.10.2    Multi1        192.10.10.2        -        2               2
192.20.20.2    Multi2        192.20.20.1      02:30      2               0
192.30.30.2    Multi3        192.30.30.1      00:50      3               2
202.30.30.2    Multi4        202.30.30.2        -       (3)              0       Q
210.40.40.2    Multi5        210.40.40.1      03:15      3               3       L
>
```

（2） グループ情報

show ip igmp groups を実行し，Group Address 内のグループを確認してください。存在しない場合，次のことを確認してください。

● そのグループメンバ（ホスト）が IGMP-Report を広告していない可能性があります。ホストを調査してください。

● 本装置の IGMP インタフェースのバージョンとホストの IGMP バージョンを確認して，ホストと接続可能であることを確認してください。

● ホストが IGMPv3 Query を無視する場合，IGMPv3 は使用できません。当該インタフェースの IGMP バージョンを 2 に設定してください。

図 6-46　show ip igmp groups コマンドの実行結果

```
> show ip igmp groups brief
Total: 7 groups
Group Address    Interface        Version  Mode       Source Count
224.1.1.1         Multi1             2        -              0
232.1.1.2         Multi1             2        -              2
234.1.1.1         Multi3             2     EXCLUDE            1
234.1.1.2         Multi3             3     INCLUDE            1
232.1.1.1         Multi4             3     INCLUDE            1
232.1.1.3         Multi4             3     INCLUDE            2
235.1.1.1         Multi4             3     EXCLUDE            3
>
```

6.6　IPv6 ネットワーク状態の確認

本節では，コンフィグレーションコマンド ip で IPv6 アドレスを指定しているインタフェースの確認について説明します。

6.6.1　当該宛先アドレスとの通信可否を確認する

IPv6 ネットワークに接続している本装置のインタフェースについて，通信相手となる装置に対して通信できるかどうかを，ping ipv6 コマンドを実行して確認してください。

図 6-47　ping ipv6 コマンドの実行結果（通信可の場合）

```
> ping ipv6 3ffe:501:811:ff01::1
PING6 (56=40+8+8 Bytes) 3ffe:501:811:ff01::10 -->3ffe:501:811:ff01::1
16 bytes from 3ffe:501:811:ff01::1, icmp_seq=0 ttl=255 time=0.286 ms
16 bytes from 3ffe:501:811:ff01::1, icmp_seq=1 ttl=255 time=0.271 ms
16 bytes from 3ffe:501:811:ff01::1, icmp_seq=2 ttl=255 time=0.266 ms
^C
--- 3ffe:501:811:ff01::1 ping6 statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.266/0.274/0.286 ms
>
```

図 6-48　ping ipv6 コマンドの実行結果（通信不可（経路あり）の場合）

```
> ping ipv6 3ffe:501:811:ff01::1
PING6 (56=40+8+8 bytes) 3ffe:501:811:ff01::10 --> 3ffe:501:811:ff01::1
^C
--- 3ffe:501:811:ff01::1 ping6 statistics ---
12 packets transmitted, 0 packets received, 100% packet loss
>
```

図 6-49　ping ipv6 コマンドの実行結果（通信不可（経路なし）の場合）

```
> ping ipv6 3ffe:501:811:ff01::1
PING6 (56=40+8+8 bytes) 3ffe:501:811:ff01::10 --> 3ffe:501:811:ff01::1
ping6: UDP connect: No route to host
>
```

6.6.2　当該宛先アドレスまでの経路を確認する

traceroute ipv6 コマンドを実行して，IPv6 ネットワークに接続している本装置のインタフェースから通信相手となる装置までの中継装置を確認してください。

図 6-50　traceroute ipv6 コマンドの実行結果

```
> traceroute ipv6 3ffe:501:811:ff01::1 numeric
traceroute6 to 3ffe:501:811:ff01::1 (3ffe:501:811:ff01::1), 30 hops max, 40 byte
packets
1  3ffe:501:811:ff03::10  0.612 ms  0.541 ms  0.532 ms
2  3ffe:501:811:ff02::5  0.905 ms  0.816 ms  0.807 ms
3  3ffe:501:811:ff01::1  1.325 ms  1.236 ms  1.227 ms
>
```

6.6.3　隣接装置との NDP 解決情報を確認する

IPv6 ネットワークに接続する本装置の回線や回線内のポートに IPv6 アドレスを設定したあとに，show ipv6 neighbors コマンドを実行し，本装置と隣接装置間のアドレス解決をしているか（NDP エントリ情報があるか）どうかを確認してください。アドレス解決をしていない場合は，「8.8.1　通信ができない，または切断されている」を参照してください。

6.6.4　フィルタリング機能を確認する

本装置でフィルタリング機能を使用した場合の確認内容には次のものがあります。

(1)　運用中の確認

(a)　統計情報の確認

show filter-flow コマンドを実行してフローフィルタ統計情報を表示し，廃棄されているパケット数を確認してください。廃棄パケット数が多い場合，本来はパケット廃棄をしてはいけない通信かもしれません。現在のネットワークの運用状況を確認してください。

図 6-51　フィルタリングによるパケット廃棄数表示

```
> show filter-flow interface tokyo1 detail
<Filter IPv6 List No.>: 40010
      Using Interface:tokyo1/in
      ip source: any
      ip destination: 3ffe:501:811:ff00::0 - 3ffe:501:811:fffe::ffff
      protocol:6(tcp)
      port source:80
      forward packets                                  :             7469982
<Filter IPv6 List No.>: 41000
      Using Interface:tokyo1/in
      ip source: any
      ip destination: any
      protocol:ip
      drop packets                                     :           327032706
 (以下省略)
>
```

6.6.5　ポリシールーティング機能を確認する

本装置でポリシールーティング機能を使用した場合の確認内容には次のものがあります。

(1)　コンフィグレーション設定後の確認

(a)　入力先インタフェースの設定確認

show ipv6 local policy コマンドを実行し，入力先インタフェースの現在のポリシールーティング条件がコンフィグレーションコマンド flow filter で設定されている内容であることを確認してください。

図 6-52　入力先インタフェースの動作状態表示

```
> show ipv6 local policy interface tokyo
<Interface Name>: tokyo <Filter List No.> 40001
        forward packets
        protocol                 : ip
        ip_source                : 3ffe:10::2 - 3ffe:10::30
        ip_destination           : 3ffe:20::2 - 3ffe:20::50
        current policy route
          Policy Group Name        route1
          Output Interface         tokyo1
          Next Hop IP address      3ffe:31::10
<Interface Name>: tokyo <Filter List No.> 40002
        forward packets
        protocol                 : ip
        ip_source                : 3ffe:101::1 - 3ffe:101::ff
        ip_destination           : 3ffe:201::1 - 3ffe:201::5f
        current policy route
          Policy Group Name        route2
          Output Interface         yokohama
          Next Hop IP address      3ffe:200::10
(以下省略)
>
```

(2) 運用中の確認

(a) 出力先インタフェースの状態確認

show ipv6 cache policy コマンドを実行し，出力先インタフェースの動作状態が UP であることを確認してください。

図 6-53　出力先インタフェースの動作状態表示

```
> show ipv6 cache policy route1
<Policy Group Name>:     route1
       priority  Interface Name  status   Nexthop
   *>      1     tokyo1            Up     3ffe:31::10
           2     tokyo1            Up     3ffe:32::10
           3     tokyo2            Down    3ffe:33::10
           4     tokyo3            Down    3ffe:30::10    default
>
```

6.6.6　Null インタフェースを確認する

本装置で Null インタフェースの機能を使用した場合の確認内容には次のものがあります。

(1) コンフィグレーション設定後の確認

(a) 経路情報の確認

show ipv6 route コマンドを実行し，コンフィグレーションコマンド static で定義した経路情報の設定内容が正しく反映されているかどうかを確認してください。

図 6-54　NULL インタフェース経路情報表示

```
> show ipv6 route static
Total: 1 routes
Destination                                  Next Hop
      Interface      Metric   Protocol  Age
3fe:501:811:ffcc::/64                       *----
      null           0/0      Static    16s
>
```

(2) 運用中の確認

(a) パケット廃棄数の確認

show ipv6 interface コマンドを実行し，Null インタフェースでパケットが廃棄されているかどうかを確認してください。

図 6-55　Null インタフェースパケット廃棄数表示例

```
> show ipv6 interface delete-packets null-interface
Interface Name:null
Discard Packets(IPv6) :92(pkts)
>
```

6.6.7　ロードバランスで使用する選択パスを確認する

(1) コンフィグレーション設定後の確認

(a) 経路情報の確認

show ipv6 route コマンドを実行し，定義したマルチパス経路の設定内容が正しく反映されているかどうかを確認してください。

図 6-56 マルチパスの経路情報表示

```
> show ipv6 route
Total: 4 routes
Destination                                      Next Hop
      Interface      Metric   Protocol  Age
::1/128                                          ::1
      localhost      0/0      Direct    51m 45s
3ffe::/64                                        fe80:11::1
      Office1        0/0      Static    50m 30s
                                                 fe80:12::1
      Office2         -         -         -
                                                 fe80:13::1
      Office3         -         -         -
                                                 fe80:14::1
      Office4         -         -         -
fe80::/64                                        fe80:20::1
      Office5        0/0      Direct    51m 27s
fe80:20::1/128                                   ::1
      localhost      0/0      Direct    50m 30s 29s
>
```

(b) 当該宛先アドレスとの通信可否を確認する

ロードバランスで使用する本装置のインタフェースについて，通信相手となる装置に対して通信できるかどうかを，ping ipv6 <IPv6 Address> specific-route source <Source Address> コマンドを実行して確認してください。ping ipv6 コマンドの <Source Address> にはロードバランスで使用する本装置の IPv6 アドレスを指定してください。

6.6.8 IPv6 DHCP サーバ機能を確認する

本装置で，DHCP サーバ機能を設定した場合の確認内容には次のものがあります。

(1) コンフィグレーション設定時の確認

(a) ネットワーク確認

本装置の DHCP サーバ機能は，IPv6 DHCP クライアント直結の構成と IPv6 DHCP リレーエージェントを経由する構成をサポートします。

(b) 設定した配布プレフィックス数の確認

本装置で配布・管理可能なプレフィックス数は 8192 です。show ipv6 dhcp server statistics コマンドを実行し，コンフィグレーションコマンド dhcp6-server host の prefix で設定した配布プレフィックス数を確認してください。

図 6-57 設定配布プレフィックス数表示例（100 個設定の場合）

```
> show ipv6 dhcp server statistics
   < DHCP Server use statistics >
     prefix pools          :100
     automatic bindings    :0
     manual    bindings    :0
(以下省略)
>
```

(2) 運用中の確認

(a) 配布済みプレフィックス数の確認

実際にクライアントへ配布したプレフィックス数については，show ipv6 dhcp server statistics コマンドを実行し，下線部の数を加算することで確認してください。

図 6-58　配布済みプレフィックス数表示例

```
> show ipv6 dhcp server statistics
   < DHCP Server use statistics >
     prefix pools           :40
     automatic bindings     :50
     manual bindings        :10
(以下省略)
>
```

(b) 配布済みプレフィックスの確認

配布したプレフィックスは，show ipv6 dhcp binding コマンドにより確認できます。

図 6-59　配布済みプレフィックスの表示例

```
> show ipv6 dhcp binding
<Prefix>             <Lease expiration>  <Type>
3ffe:1234:5678::/48      infinity            Automatic
3ffe:aaaa:1234::/48      03/04/01 11:29:00   Automatic
>
```

図 6-60　配布済みプレフィックスの表示例 (詳細)

```
> show ipv6 dhcp binding detail
<Prefix>             <Lease expiration>  <Type>
  <DUID>
3ffe:1234:5678::/48      infinity            Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
3ffe:aaaa:1234::/48      03/04/01 11:29:00   Automatic
  00:01:00:01:aa:bb:cc:dd:ee:66:77:88:99:aa
>
```

(c) プレフィックスを配布したクライアントへの経路情報の確認

本装置 DHCP サーバは，コンフィグレーションコマンドによって”dhcp6-server static-route-setting”を定義することで，プレフィックスを配布したクライアントへの経路をスタティック経路として自動的に設定します。

図 6-61　クライアントへの経路情報の確認

```
> show ipv6 route -s
Total: 10routes
Destination              Next Hop       Interface         Metric  Protocol  Age
3ffe:1234:5678::/48      ::1            tokyo             0/0      Static   45m
        <Active Gateway Dhcp>
3ffe:aaaa:1234::/48      ::1            osaka             0/0      Static   23m
        <Active Gateway Dhcp>
 :
>
```

プレフィックスを配布したクライアントへ経路情報を自動設定させる場合は，コンフィグレーションに”dhcp6-server static-route-setting”を設定してください (「コンフィグレーションコマンドレファレンス Vol.1　14. IPv6 DHCP サーバ情報」参照)。なお，本装置 DHCP サーバで自動設定した経路情報は，下記の手順で削除してください。

(1)clear ipv6 dhcp binding コマンドによって配布情報を削除する。

(2) コンフィグレーションから対象のプレフィックスの配布定義を削除する。

(3) コンフィグレーションから dhcp6-server static-route-setting を削除する。

(4) クライアントが配布をうけたプレフィックスを解放する。

(3) コンフィグレーション変更時の対応

本装置 DHCP サーバでは，コンフィグレーションを変更した場合に送信するよう定義されている DHCP

メッセージタイプ”Reconfigure”をサポートしていません。したがって本装置のコンフィグレーションを変更し適用するためには，接続されるクライアント装置のクライアント機能のリセット，またはクライアント装置の再起動が明示的に必要となります。ただし，これらを実施しなかった場合でも，初期設定（新たにプレフィックスを要求してくる）を試みます。これにより，コンフィグレーション変更内容がクライアントに反映されます。

（4） DUID(DHCP Unique Identifier) について

本装置 DHCP サーバは，初回導入時に自装置の DUID を自動生成します。DUID は装置で静的に保持しなければならないため，本装置は生成した DUID を MC 内に保存します。

（a） DUID 保存場所

本装置 DHCP サーバは，生成した DUID を PrimaryMC 上の”/primaryMC/usr/var/dhcp6/dhcp6s_duid”に保存します。

（b） DUID 確認方法

本装置 DHCP サーバの自装置の DUID は，show ipv6 dhcp server statistics コマンドで確認できます。

図 6-62　自装置 DUID の確認

```
> show ipv6 dhcp server statistics
   < Server Duid >
     00:01:00:01:3e:00:2e:5e:11:22:33:44:55:66
>
```

（5） DUID の性質に伴う導入に際しての注意

（a） 初期導入時

DHCP では DUID を装置ごとにユニークな値に設定しなければならない点に注意してください。本装置 DHCP サーバは初期導入時にだけ，インタフェースの MAC アドレスと時刻（時，分，秒）を使用して DUID を自動生成します。そのため本装置間または他社製品間で同一になることはほとんどありません。ただし，同一ネットワークで併用する他装置で DUID が本装置の DUID と同じ値になった場合は，どちらかの DUID を変更してください。

（b） copy mc コマンドによる運用

DUID の保存ファイルは，copy mc コマンドによってバックアップ MC へコピーされます。この場合，作成されたバックアップ MC を使って，現在サービス中の本装置と同一ネットワーク上に，別の本装置を IPv6 DHCP サーバとして設置する場合は，DUID 保存ファイルを削除してから実施してください。削除は erase ipv6-dhcp server duid コマンドを使用します。

図 6-63　DUID 保存ファイルの削除 (”erase ipv6-dhcp server duid”使用時)

```
> erase ipv6-dhcp server duid
>
```

（c） 他社製品とのリプレース

本装置 DHCP サーバは他社製品とのリプレースを行う場合に，DUID を他社製品で使用していた値に再設定することはできません。リプレースによるネットワーク構築の際は，必ずクライアント装置またはクライアント機能を再起動してください。

（6） 本装置を同時に 2 台以上使用する場合の注意

本装置を 2 台以上使用する場合，それぞれに同じプレフィックスの配布設定をすると，配布先のインタ

フェースに接続した，2 台以上の異なるクライアントに対して，装置ごとに同じプレフィックスを配布することがあります。これはコンフィグレーションにおいて，dhcp6-server interface に対し，preference サブコマンドに優先度を設定することで，回避可能です。ただし，コンフィグレーションコマンドで dhcp6-server interface rapid-commit を定義した場合，またはクライアントの実装が以下のどれかに該当する場合は，本値を無視することがあります。

1. クライアントによる最初の SOLICIT メッセージ送信後のサーバ応答メッセージ監視時間が，本装置がクライアントを探すために実施する NDP の応答時間よりも短く設定されている。
2. preference を無視する実装である。

現象の発生を確認した場合や，上記条件に一致する場合は，2 台以上の装置を同時に運用する構成を止めるか，または，それぞれに異なるプレフィックスの配布設定をしてください。

(7) 本装置の DHCP サーバを使用した場合のプレフィックス配布能力に関する注意

本装置の DHCP サーバを使用した場合のプレフィックス配布能力を下の表に示します。

各クライアントはリース時間の約半分でリース更新を行うため，本装置でのリース時間設定は最低でも表に示した時間の 2 倍以上，長い値で設定することを推奨します。

表 6-1　プレフィックス配布時間（すべてのプレフィックスを配布するのに要する時間）

RM CPU 使用率	クライアント数		
	1000	4000	8000
100%	15 秒	45 秒	90 秒
50%	15 秒	45 秒	90 秒
25%	15 秒	45 秒	120 秒

注　RM CPU 使用率は DHCP サーバが占有している使用率です。使用条件やコンフィグレーション内容により配布時間が異なる可能性があります。また，実際に全クライアントから配布要求を行った場合，一度に処理しきれずにクライアントで再送を行い，結果として配布時間が上記より延びます。

測定条件：
static-route-setting あり
host 定義数 8192 ／ 8192 プレフィックス（DUID 自動割り当て）
rapid-commit 指定なし

使用装置：
SB-7808R-AC

6.6.9　トンネルインタフェース情報を確認する

本装置でトンネルインタフェースを使用した場合の確認内容には次のものがあります。

(1) 動作状態の確認

show ipv6 interface コマンドを実行し，次の観点でトンネルインタフェースの状態を確認してください。

- 表示結果の physical address で示すアドレスが，本装置のトンネルインタフェース以外のインタフェースに設定されているアドレスであることを確認してください。アドレスが間違っている場合には，正しいアドレスに変更してください。
- 表示結果の physical address で示すアドレスが設定されているインタフェースの状態が UP していることを確認してください。

図 6-64　トンネルインタフェース状態表示

```
> show ipv6 interface TokyoOsakaT
TokyoOsakaT: flags=80b1<UP,POINTtoPOINT,NOTRAILERS,NOARP,MULTICAST>
        mtu 1280
        inet6 3ffe:1234:5678:9abc::64 --> fec0:1234:5678:9abc::64
        physical address inet 192.168.100.1/24 --> 192.168.100.2
>
```

（2） 通信の確認

トンネル情報で設定した自アドレス・宛先アドレスに対して，本装置および接続先装置から ping，ping ipv6 コマンドを実行し，到達性を確認してください。もし，到達性がない場合は次の対応を行ってください。

- どちらの装置からも到達性がない場合
  経路情報に問題があると考えられます。「8.8.1　通信ができない，または切断されている」を参照してください。
- 一方の装置から到達性がない場合
  中継経路間にアドレス変換装置がないかネットワーク構成を確認してください。アドレス変換装置を使用している場合は禁止構成に該当しますので，トンネルを設定する中継経路間にアドレス変換装置を設置しないようにネットワーク構成を変更してください（禁止構成については「解説書 Vol.1　12.11.4 トンネル機能使用時の注意事項」を参照してください）。

（3） 到達経路の確認

トンネルインタフェースに設定した接続先アドレスの到達経路を，show netstat routing-table numeric，show ipv6 interface，および show ip interface を実行して確認してください。経路の中継先が，本装置の別のトンネルインタフェースであった場合，禁止構成である多重トンネルとなっていることが考えられます。経路制御の設定を変更して，トンネルインタフェース以外が中継先となるように変更してください。

図 6-65　トンネルインタフェース状態表示

```
> show ipv6 interface TokyoOsakaT
TokyoOsakaT: flags=80b1<UP,POINTtoPOINT,NOTRAILERS,NOARP,MULTICAST>
        mtu 1280
        inet6 3ffe:1234:5678:9abc::64 --> fec0:1234:5678:9abc::64
        physical address inet 192.168.100.1/24 --> 192.168.100.2
> show netstat routing-table numeric
Routing tables
Internet:
Destination        Gateway          Flags    Refs    Use  Interface
 (途中省略)
192.168.100/24     link#3           UC/DMA      0      0  TokyoNagoyaT
 (途中省略)
> show ip interface TokyoNagoyaT
TokyoOsakaT: flags=80b1<UP,POINTtoPOINT,NOTRAILERS,NOARP,MULTICAST>
        mtu 1280
        inet 192.168.100.1 --> 192.168.100.2
        physical address inet6 fe80::1/64 --> fe80::2
>
```

6.7 IPv6 ユニキャストルーティング情報の確認

6.7.1 宛先アドレスへの経路を確認する

本装置で IPv6 ユニキャストルーティング情報を設定した場合は，show ipv6 route コマンドを実行して宛先アドレスへの経路が存在していることを確認してください。存在しない場合は，「6.7.2　RIPng のゲートウェイ情報を確認する」～「6.7.6　IPv6 アドレス情報が正しく配布されているかを確認する」について確認してください。

図 6-66　show ipv6 route コマンドの実行結果

6.7.2 RIPng のゲートウェイ情報を確認する

本装置の IPv6 ユニキャストルーティング情報で RIPng 機能を設定した場合は，show ipv6 rip gateway を実行して，次のことを確認してください。

- Gateway Address 内に当該経路を広告すべき隣接ルータが存在するか確認してください。存在しない場合，隣接ルータから RIPng パケットを受信していません。隣接ルータまたは隣接ルータと接続されたインタフェースを調査してください。
- Age が 30 秒以内になっていることを確認してください。30 秒以上になっている場合，隣接ルータから周期的に RIPng パケットが到達していません。隣接ルータまたは隣接ルータと接続されたインタフェースを調査してください。
- Flags に Format が表示されていないか確認してください。Format が表示されている場合，隣接ルータから不正な RIPng パケットを受信しています。隣接ルータを調査してください。
- Flags に Reject が表示されていないか確認してください。Reject が表示されている場合，当該ルータからの RIPng パケットの受信が拒否状態となっています。コンフィグレーションの ripng コマンド（interface 指定）で当該インタフェースに ripin パラメータを指定してください。
- Flags に ImportRestrict が表示されていないか確認してください。ImportRestrict が表示されている場合，インポートフィルタにより当該経路の取り込みがフィルタリングされている可能性があります。コンフィグレーションのインポートフィルタを調査してください。
- その他の場合，隣接ルータが当該経路を広告していない可能性があります。隣接ルータを調査してください。

図 6-67 show ipv6 rip gateway コマンドの実行結果

```
> show ipv6 rip gateway
Gateway Address                    Age        Flags
fe80::2a0:c9ff:fe6b:8e1b%Office01   5s        <Accept>
fe80::200:87ff:fed0:e261%Office02   8s        <Accept>
fe80::260:8ff:fe8e:3090%Office03   12s        <Accept>
     :
>
```

6.7.3 OSPFv3 のインタフェース情報を確認する

本装置の IPv6 ユニキャストルーティング情報で OSPFv3 機能を設定した場合は，show ipv6 ospf interface <Interface Name> または show ipv6 ospf interface detail を実行して，次のことを確認してください。

- Neighbor List 内に当該経路を広告すべき隣接ルータが存在するか確認してください。存在しない場合，隣接ルータから Hello パケットを受信していません。隣接ルータまたは隣接ルータと接続されたインタフェースを調査してください。
- インタフェースの状態が DR または P to P の場合，Neighbor List 内の全隣接ルータ状態が Full となっていることを確認してください。
  - Full でない場合，隣接ルータとの隣接関係が確立していません。隣接ルータを調査してください。
- インタフェースの状態が BackupDR または DR Other の場合，Neighbor List 内より DR となる隣接ルータが存在するか確認してください。
  - DR が存在し，DR の隣接ルータ状態が Full でない場合，DR との隣接関係が確立していません。隣接ルータを調査してください。
  - DR が存在しない場合は，自装置および隣接ルータの priority が設定されていない可能性があります。自装置および隣接ルータの priority を確認してください。

図 6-68 show ipv6 ospf interface コマンドの実行結果

```
> show ipv6 ospf interface Office00
Domain: 1
Area: 0.0.0.0
Interface ID: 2, Link Local Address: fe80::1000:00ff:fe00:0001%Office00
    IPv6 Address: 3ffe:501:ffff::1/64
    MTU: 1460, DDinPacket: 70, LSRinPacket: 117, ACKinPacket:70
    Router ID: 172.16.1.1, Network Type: Broadcast, State: Backup DR
    DR: 172.17.1.1, Backup DR: 172.16.1.1
    Priority: 1, Cost: 1, Instance: 0
    Intervals:
        Hello: 10s, Dead Router: 40s, Retransmission: 5s, Delay: 1s

   Neighbor List (1):
    Address                     State        Router ID         Priority
    fe80::1000:00ff:fe00:2002   Full         172.16.10.11         1
>
```

6.7.4 BGP4+ のピアリング情報を確認する【OP-BGP】

本装置の IPv6 ユニキャストルーティング情報で BGP4+ 機能を設定した場合は，show ipv6 bgp neighbors を実行して，次のことを確認してください。

- BGP Status が Established 状態となっていることを確認してください。Established 状態以外の場合，相手 BGP4+ スピーカとのピアリングが確立していません。相手 BGP4+ スピーカとの通信が可能か ping ipv6 コマンドなどで調査してください。不可能な場合，自装置と相手 BGP4+ スピーカ間のインタ

フェースまたはルータが障害となっている可能性があります。traceroute コマンドなどで障害部位を特定し，障害部位を調査してください。可能な場合，相手 BGP4+ スピーカを調査してください。

- BGP Status が Established 状態の場合，相手 BGP4+ スピーカが当該経路を広告していない可能性があります。相手 BGP4+ スピーカを調査してください（相手 BGP4+ スピーカが当該経路情報を広告しているかどうかは，show ipv6 bgp コマンドで確認できます)。

図 6-69　show ipv6 bgp neighbors コマンドの実行結果

```
> show ipv6 bgp neighbors 3ffe:501:ffff:5::2
BGP4+ Peer: 3ffe:501:ffff:5::2, Remote AS: 300
Remote Router ID: 192.168.22.10, Policy Group: 1
Description: Tokyo-Center IPv6
BGP4+ Status: Established         HoldTime: 90
    Established Transitions: 1      Established Date: 2001/08/21 19:41:01
    BGP4+ Version: 4                Type: External
    Local Address: 3ffe:501:ffff:5::1
    Local AS: 500
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 10:39:30  Last Keep Alive Received: 10:40:01
    Graceful Restart: Both
     Restart Status : Receiving   2004/07/08 17:01:23
     Receive Status : Finished    2004/07/07 10:11:12
      Stale Routes Retain Time: 300
    NLRI of End-of-RIB Marker: Advertised and Received
    BGP4+ Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                   1          7          61         68
    BGP4+ Capability negotiation: <GracefulRestart>
      Send   : <IPv6-uni, GracefulRestart(RestartTime:120s)>
      Receive: <GracefulRestart(RestartTime:300s, IPv6-uni)>
    Authentication: TCP MD5
    No fast fallover : configured
>
```

6.7.5　IS-IS の隣接情報を確認する【OP-ISIS】

本装置の IPv6 ユニキャストルーティング情報で IS-IS 機能を設定した場合は，show isis adjacency を実行し，次のことを確認してください。

- Adjacencys 内に当該経路を広告すべき隣接ルータが存在するか確認してください。存在しない場合，隣接ルータから Hello パケットを受信していません。隣接ルータまたは隣接ルータと接続されたインタフェースを調査してください。
- State が Up 状態となっていることを確認してください。Up 状態以外の場合，隣接ルータが本装置を認識していません。隣接ルータを調査してください。
- State が Up 状態の場合，隣接ルータが当該経路を広告していない可能性があります。隣接ルータを調査してください（隣接ルータが当該経路情報を広告しているかどうかは，show isis database コマンドで確認できます)。

図 6-70　show isis adjacency コマンドの実行結果

```
> show isis adjacency detail
Level-1 adjacencies
Interface: Office1, Interface Type: Broadcast
    System ID: 0000.87c0.3655, Type: IS, State: Up
    Speaks: IPv6
    Area: 49
    Circuit ID: 0x04, SNPA: 00.00.87.c0.36.55
    Priority : 64, Hold Timer: 9s, Established Time: 2003/07/01 15:30:00
    Interface Address: 192:168:7::2
>
```

6.7.6 IPv6 アドレス情報が正しく配布されているかを確認する

本装置から端末へ IPv6 アドレス情報が RA によって配布されているかどうかを確認します。

(1) 端末へアドレス情報を正しく配布しているか確認する

show ipv6 routers interface を実行して，次のことを確認してください。

- 配布すべきプレフィックスが出力されていることを確認してください。
- インタフェースが存在していることを確認してください。存在しない場合，RA の設定またはインタフェースに配布すべきプレフィックスが設定されていない可能性があります。RA またはインタフェースの IPv6 アドレスのコンフィグレーションを確認してください。

図 6-71 show ipv6 routers interface コマンドの実行結果

```
>show ipv6 routers interface Office01
Index: 2, Name: Office01
Statistics:
RSin(wait): 0(0), RAout: 0, RAin(invalid): 4(0)
Intervals:
Advertise: 200-600s (next=219s later), Lifetime: 1800s
ReachableTime: ---, RetransTimer: ---
ManagedFlag: off, OtherFlag: off, Hoplimit: 64, AdvLinkOpt: on, AdvLinkMTU: --

Prefix(origin)                     ValidLife[s] PrefLife[s] OnLink Autonomous
3ffe:2::/64(RAconf)                2592000      604800      on     on
3ffe:1111:2222:3333::/64(IFconf) 2592000      604800      on     on
>
```

(2) 本装置 - 端末間の疎通を確認する

端末側から本装置へ ping ipv6 コマンドを実行して，到達性のあることを確認してください。通信不可（到達経路なし）の場合，配布されたプレフィックスが端末に設定されていない可能性がありますので端末を調査してください。

6.8　IPv6 マルチキャストルーティング情報の確認【OP-MLT】

6.8.1　宛先グループアドレスへの経路を確認する

本装置で IPv6 マルチキャストルーティング情報の設定を行った場合は，show ipv6 mcache コマンドと netstat multicast コマンドを実行して宛先アドレスへの経路が存在していることを確認してください。存在しない場合，および downstream が正しくない場合は，「6.8.2　PIM-SM 情報を確認する」と「6.8.3　MLD 情報を確認する」について確認してください。

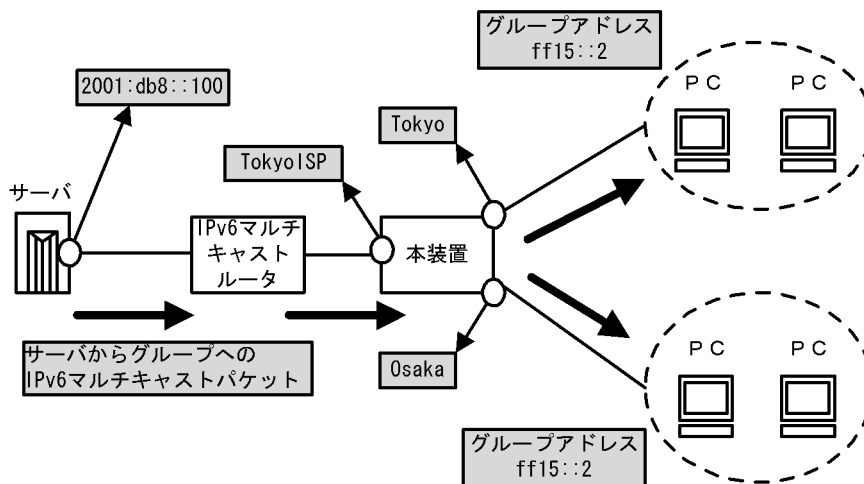
show ipv6 mcache コマンドは IPv6 マルチキャストルーティングデーモンが保持している IPv6 マルチキャストルーティングキャッシュを表示し，netstat multicast コマンドはハードウェアに登録しているマルチキャストルーティングキャッシュを表示します。

なお，netstat multicast コマンドではネガティブキャッシュ (出力インタフェースが存在しないパケット廃棄エントリ) も表示します。

図 6-72　show ipv6 mcache コマンドの実行結果

```
> show ipv6 mcache
Total:1route
Group                                   Source
ff15::2                                 2001:db8::100
    upstream:
        TokyoISP
    downstream:
        Tokyo
        Osaka
    Uptime 00:20  Expires 02:40
```

図 6-73　netstat multicast コマンドの実行結果

```
> netstat multicast
Virtual Interface Table is empty

Multicast Forwarding Cache is empty

IPv6 Virtual Interface Table
 Mif   Rate   PhyIF           Pkts-In   Pkts-Out
   0      0   reg0                  0          0
   1      0   TokyoISP              0          0
   2      0   Tokyo                 0          0
   3      0   Osaka                 0          0

IPv6 Multicast Forwarding Cache
 Origin                 Group           Packets Waits In-Mif Out-Mifs
 2001:db8::100          ff15::2               0     0    1    2  3

Total no. of entries in cache: 1
```

6.8.2 PIM-SM 情報を確認する

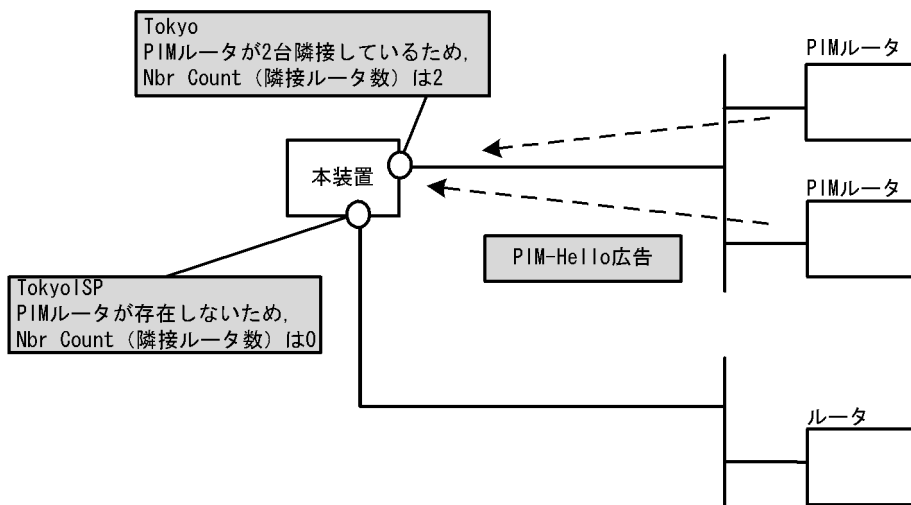
本装置の IPv6 マルチキャストルーティング情報で，PIM-SM 機能を設定した場合の確認内容には次のものがあります。

(1) インタフェース情報

show ipv6 pim interface を実行して，次のことを確認してください。

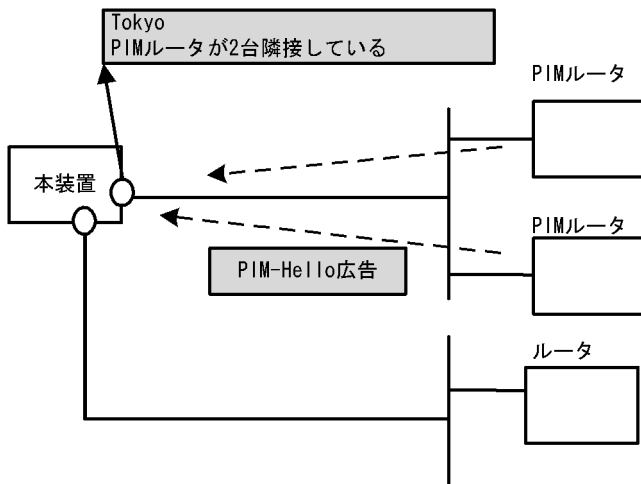
図 6-74 show ipv6 pim interface コマンドの実行結果

```
> show ipv6 pim interface
Interface     Component  Vif    Nbr    Hello    DR                          This
                                Count  Intvl    Address                     System
Tokyo         PIM-SM     1      2      30       fe80::200:87ff:fe10:a95a Y
(以下省略)
>
```

- 当該インタフェース名称が含まれていることを確認してください。当該インタフェース名称が含まれていない場合，そのインタフェースで IPv6 PIM-SM は動作していません。コンフィグレーションで当該インタフェースで IPv6 PIM が enable になっているか確認してください。また，そのインタフェースに障害が発生していないか確認してください。
- 該当インタフェースの Nbr Count（PIM 隣接ルータ数）を確認してください。0 の場合は隣接ルータが存在しないか，隣接ルータが PIM-Hello を広告していない可能性があります。隣接ルータを調査してください。

(2)　隣接情報

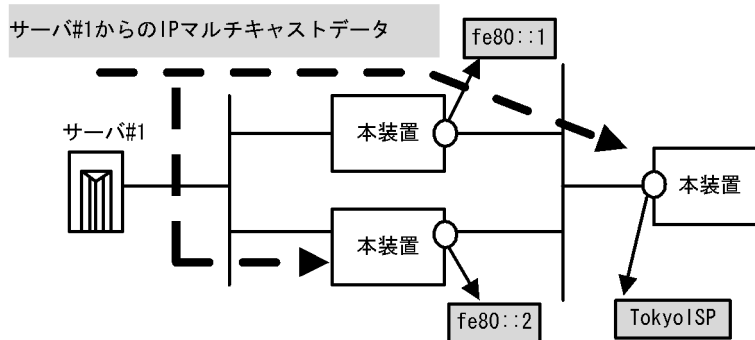
show ipv6 pim neighbor を実行して，当該インタフェースに関する隣接相手を確認してください。ある特定の隣接が存在しない場合，隣接ルータが PIM-Hello を広告していない可能性があります。隣接ルータを調査してください。

図 6-75　show ipv6 pim neighbor コマンドの実行結果

```
> show ipv6 pim neighbor
NeighborAddress          Interface Uptime Expires
fe80::200:87ff:fea0:abcd Tokyo     00:05  01:40
fe80::200:87ff:feb0:1234 Tokyo     00:05  01:40
(以下省略)
>
```

(3)　送信元ルート情報

show ipv6 rpf コマンドを実行して，送信元のルート情報を確認してください。

図 6-76　show ipv6 rpf コマンドの実行結果

```
> show ipv6 rpf
RPF Information for ? (2001:db8::100):
If multi1 NextHop fe80::1
(以下省略)
>
```

（4） PIM-SM BSR 情報

show ipv6 pim bsr を実行して，BSR アドレスが表示されていることを確認してください。”----” 表示の場合，BSR が Bootstrap メッセージを広告していないか，BSR が存在していない可能性があります。BSR を調査してください。なお，PIM-SSM では BSR は使用しないので注意してください。

図 6-77　show ipv6 pim bsr コマンドの実行結果

```
> show ipv6 pim bsr
Status: Not Candidate Bootstrap Router
BSR Address:2001:db8::1
    Priority:100,Hash Mask length:30
    Uptime:03:00
    Bootstrap Timeout:130 seconds
>
```

（5） PIM-SM ランデブーポイント情報

show ipv6 pim rendezvous-point mapping を実行して，該当の IPv6 マルチキャストグループアドレスに対する C-RP Address が表示されていることを確認してください。表示のない場合，BSR が Bootstrap メッセージを広告していないか，ランデブーポイントまたは BSR が存在していない可能性があります。ランデブーポイントおよび BSR を調査してください。なお，PIM-SSM ではランデブーポイントは使用しないので注意してください。

図 6-78　show ipv6 pim rendezvous-point mapping コマンドの実行結果

```
> show ipv6 pim rendezvous-point mapping brief
Status: Not Candidate Rendezvous Point
Total: 2 routes, 2 group, 1 RPs
Group/masklen                       C-RP Address
ff15:100::/32                       2001:db8::1
ff15:200::/32                       2001:db8::1
>
```

（6） PIM-SM ルーティング情報

show ipv6 mroute コマンドを実行し，当該宛先アドレスへの経路が存在するかどうかを確認してください。（S,G）エントリが存在しない場合は，（*,G）エントリが存在しているかを確認してください。（*,G）が存在しない場合，および in-coming.downstream が正しくない場合は隣接ルータを調査してください。なお，PIM-SSM では（*,G）は使用しません（存在しません）。

図 6-79 PIM-SM マルチキャストルート情報の表示

```
> show ipv6 mroute
Total: 4 routes, 3 groups, 2 RPs
(S,G) 2 routes -----------------------------------------------------
Group Address                           Source Address
ff15:100::50 2001:db8::100
    Uptime 02:00  Expires 02:30  Assert 01:00  Flags F  Protocol SM
    in-coming : TokyoISP       upstream: Direct Reg-Sup: 60s
    downstream: Osaka          uptime 02:30 expires 00:40
ff15:200::1 2001:db8::200
    Uptime 02:00  Expires 02:30  Assert 01:00  Flags F  Protocol SM
    in-coming : Tokyo          upstream: Direct Reg-sup：60s
    downstream: localhost      uptime 02:30 expires--:--

(*,G) 2 routes -----------------------------------------------------
Group Address                           RP Address
ff15:100::50 2001:db8::1
    Uptime 02:00  Expires 02:30  Assert 01:00  Flags R  Protocol SM
    in-coming : Tokyo          upstream: This System
    downstream: Osaka          uptime 02:30 expires 00:40
ff15:200::1 2001:db8::2
    Uptime 02:00  Expires 02:30  Assert 01:00  Flags R  Protocol SM
    in-coming : Tokyo          upstream: fe80::1200:87ff:fe10:1234
    downstream: Osaka          uptime 02:30 expires 00:40
    downstream: Nagoya         uptime 02:30 expires 00:41
```

6.8.3 MLD 情報を確認する

本装置の IPv6 マルチキャストルーティング情報で MLD 機能を設定した場合の確認内容には次のものがあります。

(1) インタフェース情報

show ipv6 mld interface を実行して，次のことを確認してください。

- Interface 欄に表示されているインタフェースを確認してください。表示されているインタフェースで MLD が動作しています。期待したインタフェースが表示されない場合は pim6 または mld コンフィグレーションを確認してください。また，そのインタフェースに障害が発生していないか確認してください。
- 該当インタフェースの Group Count（加入グループ数）を確認してください。0 の場合は加入グループが存在しないかグループ加入ホストが MLD-Report を広告していない可能性があります。ホストを調査してください。
- Version 欄に表示されているバージョンが当該インタフェースで使用しているホストと接続可能であるか確認してください。
- Notice 欄にコードが表示される場合は MLD パケットが廃棄されています。コードから廃棄理由を調査してください。

図 6-80 show ipv6 mld interface コマンドの実行結果

```
> show ipv6 mld interface
Total: 10 Interfaces
Interface       Querier                     Expires  Version  Group Count  Notice
Tokyo           fe80::100:87ff:fe10:2959     02:30      1             4    L
Osaka           fe80::100:87ff:fe10:2959     01:30      2             2
Nagoya          fe80::100:87ff:fe10:2959      -        (2)            5    QR
Office1         fe80::1234                   01:00      1             3    Q
Office2         fe80::2592                   02:30      1             6
(以下省略)
>
```

（2） グループ情報

show ipv6 mld group を実行し，Group Address 内のグループを確認してください。存在しない場合，次のことを確認してください。

- そのグループメンバ（ホスト）が MLD-Report を広告していない可能性があります。ホストを調査してください。
- 本装置の MLD インタフェースのバージョンとホストの MLD バージョンを確認して，ホストと接続可能であることを確認してください。
- ホストが MLDv2 Query を無視する場合，MLDv2 は使用できません。当該インタフェースの MLD バージョンを 1 に設定してください。

図 6-81　show ipv6 mld group コマンドの実行結果

```
> show ipv6 mld group brief
Total: 20 groups
Group Address     Interface Version Mode    Source Count
ff15:100::50      Tokyo        1     -                 9
ff15:100::60      Osaka        2    INCLUDE            2
ff15:200::1       Osaka        1     -                 0
ff15:200::2       Nagoya       2    EXCLUDE            1
(以下省略)
>
```

6.9 MPLS 通信の確認【OP-MPLS】

6.9.1 非 VPN MPLS 通信を確認する

(1) MPLS パケットの通信を確認する

LDP または routing-base な static LSP で非 VPN MPLS 通信をする場合，宛先アドレスまでの MPLS パケットの到達性を確認できます。ping mpls コマンドにより宛先アドレスまでの MPLS パケットの到達性を確認してください。

到達性の確認が成功した例を，「図 6-82　LSP ping による MPLS パケットの到達性確認 (成功時)」に，中継装置に問題があり失敗した例を「図 6-83　LSP ping による MPLS パケットの到達性確認 (失敗時 1)」に，ping mpls コマンドを実施した装置に問題があり失敗した例を「図 6-84　LSP ping による MPLS パケットの到達性確認 (失敗時 2)」に示します。

図 6-82　LSP ping による MPLS パケットの到達性確認 (成功時)

```
> ping mpls 192.168.113.101/32
Route to 192.168.113.101/32 is via LDP FEC

S from 192.168.0.7 : seq=1  time=100.001ms  code=3(0)
S from 192.168.0.7 : seq=2  time=97.102ms   code=3(0)
S from 192.168.0.7 : seq=3  time=123.304ms  code=3(0)
S from 192.168.0.7 : seq=4  time=110.075ms  code=3(0)
S from 192.168.0.7 : seq=5  time=105.870ms  code=3(0)
^C
--- lsp ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

Sであることを確認してください

図 6-83　LSP ping による MPLS パケットの到達性確認 (失敗時 1)

```
> ping mpls 192.168.113.101/32
Route to 192.168.113.101/32 is via LDP FEC

  from 192.168.5.7 : seq=1  time=100.001ms  code=11(0)
  from 192.168.5.7 : seq=2  time=97.102ms   code=11(0)
  from 192.168.5.7 : seq=3  time=123.304ms  code=11(0)
  from 192.168.5.7 : seq=4  time=110.075ms  code=11(0)
  from 192.168.5.7 : seq=5  time=105.870ms  code=11(0)
^C
--- lsp ping statistics ---
5 packets transmitted, 5 packets received, 100% packet loss
```

Sと表示されません

図 6-84　LSP ping による MPLS パケットの到達性確認 (失敗時 2)

```
> ping mpls 192.168.113.101/32
Corresponding FEC dose not found.
```

(2) 通過ルータを確認する

LDP または routing-base な LSP で非 VPN MPLS 通信をする場合，宛先アドレスまでの通過ルータを確認できます。traceroute mpls コマンドにより宛先アドレスまでの通過ルータを確認してください。

通過ルータの確認が成功した例を，「図 6-85　LSP traceroute による通過ルータの確認 (成功時)」に，中

継装置に問題があり失敗した例を「図 6-86　LSP traceroute による通過ルータの確認 (失敗時 1)」に，traceroute mpls コマンドを実施した装置に問題があり失敗した例を「図 6-87　LSP traceroute による通過ルータの確認 (失敗時 2)」に示します。

図 6-85　LSP traceroute による通過ルータの確認 (成功時)

```
> traceroute mpls 192.168.113.101/32
Trace to 192.168.113.101/32 is via LDP FEC

  from 192.168.7.7 : time=100.001ms  mtu=1500  [Label: 22] code=8(0)
  from 192.168.6.7 : time=97.102ms  mtu=1500  [Label: 21] code=8(0)
  from 192.168.5.7 : time=123.304ms  mtu=1500  [implicit-null] code=8(0)
S from 192.168.0.7 : time=110.075ms  code=3(0)
```


図 6-86　LSP traceroute による通過ルータの確認 (失敗時 1)

```
> traceroute mpls 192.168.113.101/32
Trace to 192.168.113.101/32 is via LDP FEC

from 192.168.7.7 : time=100.001ms  mtu=1500  [Label: 22] code=8(0)
from 192.168.6.7 : time=97.102ms  mtu=1500  [Label: 21] code=4(0)
```


図 6-87　LSP traceroute による通過ルータの確認 (失敗時 2)

```
> traceroute mpls 192.168.113.101/32
Trace to 192.168.113.101/32 is via LDP FEC

  timeout
  timeout
  timeout
^C
```

(3) MPLS 網内 IPv4 ユニキャストルーティング情報の確認

LDP による非 VPN MPLS 通信をするためには，宛先アドレスへの経路が必要です。IPv4 ユニキャストルーティング情報を，「6.4.1　宛先アドレスへの経路を確認する」に従って確認します。

static LSP による MPLS 通信では，宛先アドレスへの経路は不要です。

(4) MPLS ラベルを確認する

非 VPN MPLS 通信をする場合，show mpls forwarding-table コマンドでラベルとフォワーディングテーブルを確認してください。

MPLS パケット送受信数の収集統計取得が開始されている場合，show mpls forwarding-table コマンドに statistics オプションを指定すると送受信パケット数が表示されます。

図 6-88 IP アドレス指定によるラベルとフォワーディング情報の表示

```
> show mpls forwarding-table 192.168.113.101/32 statistics
Current Statistics Status : Collecting
Total : 1
FEC: 192.168.113.101/32              Next Hop : 192.168.7.7
  Out:   Label:    4503              Interface: Fukuoka
           Packets         :                78901
           Octets          :             25874630
           Discard Packets :                  190
```

static LSP を使用している場合のコア LSR では，show mpls forwarding-table コマンドのパラメータに，宛先アドレスではなくラベルまたは LSPID を指定する必要があるので注意してください。

(5) Basic LDP セッションの状態を確認する

show mpls ldp コマンドで Basic LDP セッションの状態が UP であることを確認してください。LDP による非 VPN MPLS 通信を行う場合は，宛先アドレスへの経路の出力インタフェースを指定した Basic LDP セッションが UP している必要があります。

図 6-89 Basic LDP セッション状態の表示

```
> show mpls ldp
total:2
Interface Name Local           Remote          Status  Sent  Received
- -------------  --------------  ------------    ----    ------ ---------
toR2           172.16.1.1      172.16.1.2      UP         5       10
toR3           172.16.2.1      172.16.2.2      UP        11       11
```

upであることを確認してください

(6) Basic LDP セッションダウンの要因を確認する

Basic LDP セッションがダウンしている場合，show mpls ldp detail コマンドで Basic LDP セッションダウンの要因を確認してください。

図 6-90 Basic LDP セッションダウンの要因の表示

```
> show mpls ldp detail

total: 1
Interface Name : toR2
     Local:10.2.4.4         Remote:-                 Status: DOWN
     Time-since-last-LDP-status-change: 00:00:04
     Last down reason: Hello expired(0x80000009)
     Hold time: 15sec  Hello interval: 5sec
     Message               Send count  Last sent   Receive count   Last received
     Notification                   2   15:29:30               1        15:29:06
     Hello                          3   15:29:13               6        15:29:12
     Initialization                 2   15:29:11               1        15:29:11
     KeepAlive                      1   15:29:11               1        15:29:11
     Address                        1   15:29:11               1        15:29:11
     Address Withdraw               0   00:00:00               0        00:00:00
     Label Mapping                 11   15:29:25              10        15:29:11
     Label Request                  0   00:00:00               0        00:00:00
     Label Withdraw                 1   15:29:21               0        00:00:00
     Label Release                  0   00:00:00               0        00:00:00
     Label Abort Request            0   00:00:00               0        00:00:00
     Others                         0   00:00:00               0        00:00:00
```

ダウン要因

Helloメッセージの統計情報

表 6-2　Basic LDP セッションの障害解析方法

項番	確認内容・コマンド	対応
1	show mpls ldp detail コマンド表示結果の Last down reason を確認してください。	最後に Basic LDP セッションが UP から Down に変化した理由が表示されている場合は項番 3 へ。
		’-’が表示されている場合は，まだ一度も Basic LDP セッションが確立していない状態です。項番 2 へ。
2	Hello メッセージの統計情報を確認してください。	受信回数が 0 の場合，対向 LSR からの Hello メッセージが届いていません。相手ルータの状態およびリンクの状態を確認してください。
		Hello を受信している場合，Basic LDP セッションの tcp コネクションの状態および対向 LSR の状態を確認してください。
3	show mpls ldp detail コマンドの Last down reason の表示内容を確認してください。	Configuration changed or unsupported hardware の場合，コンフィグレーションが変更されたか，MPLS 未対応のハードウェアを使用しています。コンフィグレーションとハードウェアを確認してください。
		Hello expired の場合，対向 LSR からの Hello メッセージが届かなくなっています。相手ルータの状態およびリンクの状態を確認してください。
		Keepalive expired の場合，対向 LSR からの Keepalive メッセージが届かなくなっています。相手ルータの状態およびリンクの状態を確認してください。※
		Illegal message received の場合，対向 LSR から不正なメッセージを受信したことにより Basic LDP セッションを強制解放しています。※
		Notification message received の場合，対向 LSR から Notification メッセージを受信したことにより Basic LDP セッションを強制解放しています。※
		Unknown の場合，上記以外の理由で Basic LDP セッションが解放されています。※

注※　これらの要因で Basic LDP セッションが障害となった場合，通常は自動的に Basic LDP セッションが回復します。しばらく待っても Basic LDP セッションが回復しない場合は，相手ルータの状態を確認してください。

(7) static LSP の状態を確認する

show mpls static-lsp コマンドで static LSP の状態を確認してください。

図 6-91　static LSP 状態の表示

(8) ポリシールーティングの状態を確認する

policy-base の static LSP で非 VPN MPLS 通信をする場合，show filter-flow コマンドでポリシールーティング機能により MPLS 通信がされていることを確認してください。

図 6-92　MPLS ポリシールーティング指定時のフローフィルタ統計

```
> show filter-flow interface tokyo1 detail
<Filter List No.>: 10
      Using Interface:tokyo1/in
      ip source: any
      ip destination: 192.168.113.101
      policy-mpls routing
           <Ingress LSP ID>: 10000
      hit packets                          :     1234567890
```

カウンタが増えていることを確認してください

6.9.2　IP-VPN 通信を確認する

(1) 対向 LSR への非 VPN MPLS 通信の確認

MPLS による IP-VPN 通信をするためには，対向 LSR のローカルアドレス (BGP ピアの IP アドレス) 宛の非 VPN MPLS 通信ができることが必要です。「6.9.1　非 VPN MPLS 通信を確認する　(4) MPLS ラベルを確認する」を参考に，対向 LSR のローカルアドレス宛に非 VPN MPLS 通信ができることを確認してください。

(2) IP-VPN 経路情報を確認する

本装置の IPv4 ユニキャストルーティング情報で VPN 機能を設定した場合は，show ip route vpn コマンドを実行し，当該宛先アドレスへの経路が存在するかどうかを確認してください。

図 6-93　指定 VPN の経路情報の表示

```
> show ip route vpn Site-B
In VPN Site-B routing table
Total: 22 routes
Destination        Next Hop        Interface      Metric  Protocol    Age
10.1.2/24          10.1.2.100      LAN1           0/0     Direct      12d 11h
127/8              127.0.0.1       -              0/0     Static      12d 11h
127.0.0.1/32       127.0.0.1       -              0/0     Direct      12d 11h
172.30.180/24      10.1.2.92       LAN1           2/0     BGP          8d  2h
172.30.191/24      10.1.2.92       LAN1           2/0     BGP          8d  2h
172.31/16          192.168.214.21  remote-gateway 0/0     Static      10d 21h
172.32/16          192.168.214.21  remote-gateway 0/0     Static      10d 21h
192.168.1/24       10.1.2.88       LAN2           2/1     OSPF_ASE     3m 21s
192.168.3/24       10.1.2.88       LAN2           2/1     OSPF_ASE     3m 18s
192.168.11/24      10.1.3.92       Site-A         3/0     BGP_LOCAL   19h 32m
192.168.13/24      10.1.3.92       Site-A         3/0     BGP_LOCAL   19h 32m
192.168.51/24      10.1.4.32       Site-C         2/2     BGP_LOCAL    1d  2h
192.168.53/24      10.1.4.32       Site-C         2/2     BGP_LOCAL    1d  2h
192.168.200/26     192.168.216.1   remote-gateway 1/3     BGP         14m 21s
192.168.200.128/26 192.168.216.3   remote-gateway 1/3     BGP         14m 21s
192.168.220/24     172.33.215.11   remote-gateway 0/2     BGP          1h 42m
      :
```

(3) mp-BGP のピアリング情報を確認する

IP-VPN 通信を行う場合は，対向 LSR との BGP ピアリング情報で，BGP Capability パラメータのネゴシエーションに IPv4-VPN が含まれている必要があります。「6.4.4　BGP4 のピアリング情報を確認する【OP-BGP】」に従って show ip bgp neighbors コマンドを実行し，BGP Capability negotiation に IPv4-VPN が表示されていることを確認してください。また，相手の IP アドレスがローカルアドレスとなっていることも確認してください。

keep-none-vpn が指定されている場合は，VPN マップ情報でマッピングされていない VPN 情報を保持し

ません。VPN 構成の追加などで VPN 経路を再学習したい場合は，clear ip bgp コマンドを使用して当該ピアをいったん切断するか，ピアから VPN 経路を再広告させてください。

表 6-3　VPN 経路の確認事項と対応

項番	確認内容・コマンド	対応
1	BGP Capability negotiation の結果に IPv4-VPN が含まれているか確認してください。 show ip bgp neighbors xx.xx.xx.xx （xx.xx.xx.xx はアドレスを指定）	IPv4-VPN が含まれている場合は項番 2 へ。
		IPv4-VPN が含まれていない場合は，コンフィグレーションを修正してください。
2	VPN 情報の対応が正しいか，コンフィグレーションの vpnmap を確認してください。	コンフィグレーションが正しい場合は項番 3 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
3	隣接ルータが VPN 経路を広告しているか確認してください。	広告している場合は項番 4 へ。
		広告していない場合は隣接ルータを確認してください。
4	コンフィグレーションで keep-none-vpn を指定しているか確認してください。	指定している場合は clear ip bgp コマンドを使用して当該ピアをいったん切断するか，ピアより VPN 経路を再広告させてください。それでも解決しない場合は該当ルータで障害情報を収集してください。 dump protocols unicast all ※
		指定していない場合は該当ルータで障害情報を収集してください。 dump protocols unicast all ※

注※　障害情報収集コマンドを実行すると，次に示すエリアにファイルが作成されます。
格納エリア：/primaryMC/usr/var/rtm
ファイル名：rt_trace と rt_dump.gz

（4） MPLS ラベルを確認する

MPLS を利用した IP-VPN を使用する場合，show mpls forwarding-table コマンドでラベルとフォワーディングテーブルを確認してください。

show mpls forwarding-table コマンドで VPN ID を指定して，リモートサイトに対する出力ラベルと，ローカルサイトに対する入力ラベルが設定されていることを確認してください。

図 6-94　VPN ID 指定によるラベルとフォワーディング情報の表示

```
> show mpls forwarding-table vpn Site-B
Total : 1
VPN ID: Site-B
FEC: 192.168.113.101/32            Next Hop : 192.168.7.7
  Out:   Label: 1048573/1048574      Interface: Tokyo
```

（5） MPLS パケットの通信を確認する

MPLS を利用した IP-VPN を使用する場合，宛先アドレスまでの MPLS パケットの到達性を確認できます。ping mpls コマンドに vpn オプションを指定して宛先アドレスまでの MPLS パケットの到達性を確認してください。

図 6-95　LSP ping による MPLS パケットの到達性確認

```
> ping mpls 192.168.113.101/32 vpn Site-B
Route to 192.168.113.101/32 is via LDP FEC (vpn:Site-B)

S from 192.168.0.7 : seq=1  time=100.001ms  code=3(0)
S from 192.168.0.7 : seq=2  time=97.102ms   code=3(0)
S from 192.168.0.7 : seq=3  time=123.304ms  code=3(0)
S from 192.168.0.7 : seq=4  time=110.075ms  code=3(0)
S from 192.168.0.7 : seq=5  time=105.870ms  code=3(0)
^C
--- lsp ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

Sであることを確認してください

（6） 通過ルータを確認する

MPLS を利用した IP-VPN を使用する場合，宛先アドレスまでの通過ルータを確認できます。traceroute mpls コマンドに vpn オプションを指定し，宛先アドレスまでの通過ルータを確認してください。

図 6-96　LSP traceroute による通過ルータの確認

```
> traceroute mpls 192.168.113.101/32 vpn Site-B
Trace to 192.168.113.101/32 is via LDP FEC (vpn:Site-B)

  from 192.168.7.7 : time=100.001ms  mtu=1500  [Label: 22] code=8(0)
  from 192.168.6.7 : time=97.102ms  mtu=1500  [Label: 21] code=8(0)
  from 192.168.5.7 : time=123.304ms  mtu=1500  [implicit-null] code=8(0)
S from 192.168.0.7 : time=110.075ms  code=3(0)
```

通過ルータが正しいことを確認してください

最後の1行がSになっていることを確認してください

6.9.3　EoMPLS(L2-VPN) 通信を確認する

（1） 対向 LSR への非 VPN MPLS 通信の確認

MPLS による EoMPLS(L2-VPN) 通信をするためには，対向 LSR のローカルアドレス (Targeted LDP ピアの IP アドレス) 宛の非 VPN MPLS 通信ができることが必要です。「6.9.1　非 VPN MPLS 通信を確認する　(4) MPLS ラベルを確認する」を参考に，対向 LSR ローカルアドレス宛に非 VPN MPLS 通信ができることを確認してください。

（2） EoMPLS(L2-VPN) の VC の状態を確認する

運用端末から本装置に対して show mpls l2transport コマンドを実行し，VC の状態を確認してください (例は VC ID を”5”とします)。

図 6-97　show mpls l2transport コマンドの実行結果

```
>show mpls l2transport vc 5
Transport  Interface Name VC    IN       Out        Tunnel
VC ID                     State VC Label VC Label   Label
--------- ----------- ---------- ------- ---------  --------
5          office1      UP          23        26    1048576
```


（3） Targeted LDP セッション状態を確認する

EoMPLS（L2-VPN）通信を行う場合は，対向 LSR への Targeted LDP セッションが UP している必要があります。Targeted LDP セッションのピアのアドレスが相手出口エッジルータのローカルアドレスとなっていることも確認してください。

図 6-98　LDP セッション状態の表示

```
 > show mpls ldp
 total:3
   Interface Name Local           Remote          Status  Sent  Received
 - -------------- --------------- --------------- ------- ------ --------
 T (localhost)    10.3.3.3        10.1.1.1        UP         5       10
   toR2           172.16.1.1      172.16.1.2      UP         5       10
   toR3           172.16.2.1      172.16.2.2      UP        11       11
```


（4） Targeted LDP セッション Down の要因を確認する

最初に確立しない Targeted LDP セッションの相手ピアへの経路情報を確認してください。経路情報がない場合には，「8.6　IPv4 ユニキャストルーティングの通信障害」に従って障害を取り除いてください。

show mpls ldp コマンドで detail オプションを指定し，LDP セッションが確立しない原因を調査してください。LDP セッション状態表示内容を次の図に，確認内容を「表 6-4　Targeted LDP セッションの確認内容と対応」に示します。

図 6-99　LDP セッション状態の表示 (詳細)

```
> show mpls ldp  10.1.1.1 detail
Total:1
Interface Name: (localhost)  targeted
Local: 10.3.3.3          Remote: 10.1.1.1         Status: DOWN
Time-since-last-LDP-status-change: 00:25:39
Last down reason: Illegal message received(0x80000003)
Hold time: 45sec  Hello interval: 15sec
Message             Send count  Last sent  Receive count   Last received
Notification                 0  00:00:00              0        00:00:00
Hello                        5  11:15:19              5        11:15:19
Initialization               1  22:55:29              1        11:15:19
KeepAlive                    5  12:23:30              5        11:15:19
Address                      0  00:00:00              0        00:00:00
Address Withdraw             0  00:00:00              0        00:00:00
Label Mapping                0  00:00:00              0        00:00:00
Label Request                0  00:00:00              0        00:00:00
Label Withdraw               0  00:00:00              0        00:00:00
Label Release                0  00:00:00              0        00:00:00
Label Abort Request          0  00:00:00              0        00:00:00
Others                       0  00:00:00              0        00:00:00
```

ダウン要因

Helloメッセージの統計情報

表 6-4　Targeted LDP セッションの確認内容と対応

項番	確認内容・コマンド	対応
1	show mpls ldp コマンド表示結果の Last down reason を確認してください。	最後に Targeted LDP セッションが UP から Down に変化した理由が表示されている場合は項番 3 へ。
		’ -’ が表示されている場合は，まだ一度も Targeted LDP セッションが確立していない状態です。項番 2 へ。
2	Hello メッセージの統計情報を確認してください。	受信回数が 0 の場合，対向 LSR からの Hello メッセージが届いていません。相手ルータの状態および経路の状態を確認してください。 Targeted LDP セッションの Hello メッセージの宛先 IP アドレスは，本装置のローカルアドレスでなければなりません。対向 LSR での Targeted LDP セッションの Hello メッセージの宛先 IP アドレスが，本装置のローカルアドレスになっているかどうかを確認してください。
		Hello を受信している場合，Targeted LDP セッションの tcp コネクションの状態および対向 LSR の状態を確認してください。
3	show mpls ldp detail コマンドの Last down reason の表示内容を確認してください。	Configuration changed or unsupported hardware の場合，コンフィグレーションが変更されています。コンフィグレーションを確認してください。
		Hello expired の場合，対向 LSR からの Hello メッセージが届かなくなっています。相手ルータの状態および経路の状態を確認してください。
		Keepalive expired の場合，対向 LSR からの Keepalive メッセージが届かなくなっています。相手ルータの状態および経路の状態を確認してください。※
		Illegal message received の場合，対向 LSR から不正なメッセージを受信したことにより Targeted LDP セッションを強制解放しています。※
		Notification message received の場合，対向 LSR から Notification メッセージを受信したことにより Targeted LDP セッションを強制解放しています。※

項番	確認内容・コマンド	対応
		Unknown の場合，上記以外の理由で Targeted LDP セッションが解放されています。※

注※　これらの要因で Targeted LDP セッションが障害となった場合，通常は自動的に Targeted LDP セッションが回復します。しばらく待っても Targeted LDP セッションが回復しない場合は，相手ルータの状態を確認してください。

(5) VC ラベル，および Tunnel LSP ラベルを確認する

show mpls l2transport コマンドを実行して In VC Label，Out VC Label，Tunnel Label の表示を確認してください。Label 表示内容を次の図に，確認事項を「表 6-5　Label 表示内容と確認事項」に示します。

図 6-100　Label 表示内容

```
>show mpls l2transport
Total:6
  Transport  L2transport    VC     In       Out        Tunnel   Peer Address
  VC ID      Interface Name Status VC Label VC Label    Label
- ---------- -------------- ------ -------- --------   -------  ---------------
  4          office1        UP           23       26  1048576  10.1.2.2
S 16         office5        UP        20000    20000       16  -
  101        office2        DOWN         24        -        -  100.3.3.2
  106        -              DOWN          -       66       88  11.10.3.2
S 10000      office6        UP        20001    25000    10000  -
  4294967295 office99       DOWN    1048575  1048570        -  200.10.10.2
```

表 6-5　Label 表示内容と確認事項

項番	Label 表示内容	確認事項
1	In VC Label 表示が”‐”のとき	show interface コマンドを実行し，自装置側の l2transport のインタフェース回線の状態表示が”active up”になっていることを確認してください。
		自装置側のコンフィグレーションの妥当性 (VCID，L2transport Interface，Targeted peer) を確認してください。
2	Out VC Label 表示が”‐”のとき	相手装置側の l2transport 回線が UP していることを確認してください。
		相手装置側のコンフィグレーションの妥当性 (VCID，L2transport Interface，Targeted peer) を確認してください。
3	In，Out 両方の VC Label 表示が”‐”のとき	自装置と相手装置の互いのコンフィグレーションが一致 (VCID，Targeted peer) しているかどうか確認してください。
4	Tunnel Label 表示が”‐”のとき	「6.9.1　非 VPN MPLS 通信を確認する　(6) Basic LDP セッションダウンの要因を確認する」に従って原因を調査してください。
5	全ラベル表示がなされているとき	自装置と相手装置の互いのコンフィグレーションのパラメータ (line type，local/remote MTU) が一致しているかどうか確認してください。

注　表示内容が複合している場合はそれぞれに対して確認事項の内容を実行してください。

6.10　QoS 機能の確認

6.10.1　QoS 制御機能を確認する

本装置で QoS 制御機能を使用した場合，運用中の確認内容には次のものがあります。

（1）帯域制御によるパケット廃棄の確認

show qos ip-flow コマンドを実行してフロー QoS 統計情報を表示し，QoS 機能の帯域制御によって廃棄されているパケット数を確認してください。廃棄パケット数が多い場合，本来はパケット廃棄をしてはいけない通信部位の可能性があります。現在のネットワークの運用状況を確認してください。

図 6-101　フロー QoS 統計情報表示

```
> show qos ip-flow interface tokyo1 detail
<QoS IP List No.>:    1
      Using Interface:tokyo1/in
      ip source: 170.10.11.21 - 170.10.11.30
      ip destination: any
      protocol:ip
      packets of    1000000kbps and under(priority3 discard4)
                                                       :                7021
      packets of    1000000kbps over     (drop)
                                                       :                 729
<QoS IP List No.>:    2
      Using Interface: tokyo1/out
      ip source: any
      ip destination: any
      protocol:6(tcp)
      port destination:20 - 21
      ack check off
      syn check off
      hit packets                   (priority8 discard4)
                                                       :            11568793
（以下省略）
>
```

（2）キュー制御によるパケット廃棄の確認

show qos queueing コマンドを実行して出力優先度キュー情報を表示し，QoS 機能のキュー制御によって廃棄されているパケット数を確認してください。廃棄パケット数が多い場合，本来はパケット廃棄をしてはいけない通信部位の可能性があります。現在のネットワークの運用状況を確認してください。

図 6-102　出力優先度キュー情報表示

```
> show qos queueing nif 0 line 1
NIF0/Line1 (outbound), Rate_limit=1000kbps, Qmode=Priority
 Max_Queue=8
  Priority(Queue)=1, Qlen=1, Maximum_Qlen=2, Limit_Qlen=127
   Discard       send_pkt    discard_pkt      send_byte   discard_byte
   1                 6533             19         533.0k          10.0k
   2                 2564           1581         125.5M          20.0k
   3              2256877           1235        5433.2M          10.0k
   4               568788           2548         255.0k          20.0k
   total          2834762           5383        5559.6M          60.0k
（以下省略）
>
```

（3）階層化シェーパによるパケット廃棄の確認

show shaper コマンドを実行して優先度キュー情報を表示し，QoS 機能の階層化シェーパ制御によって廃棄されているパケット数を確認してください。廃棄パケット数が多い場合，本来はパケットを廃棄しては

いけない通信部位の可能性があります。現在のネットワーク運用状況を確認してください。

図 6-103 優先度キュー情報表示

```
> show shaper 0/1
NIF/Line=0/1, Rate_limit=1000000kbps
 Default_Aggregated_Queue,
 Qmode=4WFQ, Peak_rate=1000kbps, Min_rate=1000kbps, Weight=1
  Queue     send_pkt   discard_pkt   send_byte    discard_byte
  1                0             0           0               0
  2                0             0           0               0
  3                0             0           0               0
  4               11             0        1.0k               0
  total           11             0        1.0k               0

 Interface=eth0/1, Aggregated_Queue=100,
 Qmode=LLQ + 3WFQ, Peak_rate=300000kbps, Min_rate=300000kbps, Weight=1
  Queue     send_pkt   discard_pkt   send_byte    discard_byte
  1                0             0           0               0
  2             6831       4782607       10.4M            7.3G
  3                0             0           0               0
  4         14530338      33261538       22.1G           50.6G
  total     14537169      38044145       22.1G           57.9G

>
```
注 インタフェース名称が設定されている場合だけ表示されます。

6.11 高信頼性機能の確認

6.11.1 IPv4 ネットワークの VRRP の同期を確認する

本装置で VRRP の機能を使用した場合の確認内容には次のものがあります。

(1) コンフィグレーション設定後の確認

(a) 経路情報の確認

show vrrpstatus detail コマンドを実行し，コンフィグレーションコマンド virtual-router で定義した VRRP 情報の設定内容が正しく反映されているかどうかを確認してください。

図 6-104 VRRP 運用状態表示

```
> show vrrpstatus detail
Department1: VRID 1
   Virtual Router IP Address : 170.10.10.2
   Virtual MAC Address : 00-00-5e-00-01-01
   Current State : MASTER
   Admin State : enable
   Priority : 100
   IP Address Count : 1
   Master Router's IP Address : 170.10.10.2
   Primary IP Address : 170.10.10.1
   Authentication Type : SIMPLE TEXT PASSWORD
   Authentication Key : ABCDEFG
   Advertisement Interval : 1
   Preempt Mode : ON
   Virtual Router Up Time : Tue Feb 22 13:05:53 2000
   Critical Interface : Department2
   Critical Interface Status : (IF UP)
>
```

(2) 運用中の確認

(a) 仮想ルータ状態の確認

本装置および本装置と同一仮想ルータを構成する相手装置において，仮想ルータの状態が MASTER または BACKUP になっていること，および同一仮想ルータで複数のマスタルータが存在しないことを確認してください。本装置での仮想ルータの状態確認には show vrrpstatus コマンドを使用してください。

図 6-105 仮想ルータの状態表示例

```
> show vrrpstatus
Department1:VRID 1 MASTER virtual-ip 170.10.10.2 priority 150
>
```

6.11.2 IPv6 ネットワークの VRRP の同期を確認する

本装置で VRRP の機能を使用した場合の確認内容には次のものがあります。

(1) コンフィグレーション設定後の確認

(a) 経路情報の確認

show vrrpstatus detail コマンドを実行し，コンフィグレーションコマンド virtual-router で定義した VRRP 情報の設定内容が正しく反映されているかどうかを確認してください。

図 6-106　VRRP 運用状態表示

```
> show vrrpstatus detail
Department1: VRID 1
   Virtual Router IP Address : fe80::1234
   Virtual MAC Address : 00-00-5e-00-01-01
   Current State : MASTER
   Admin State : enable
   Priority : 100
   IP Address Count : 1
   Master Router's IP Address : fe80::abcd
   Primary IP Address : fe80::abcd
   Authentication Type : SIMPLE TEXT PASSWORD
   Authentication Key : ABCDEFG
   Advertisement Interval : 1
   Preempt Mode : ON
   Virtual Router Up Time : Tue Feb 22 13:05:53 2000
   Critical Interface : Department2
   Critical Interface Status : (IF UP)
>
```

(2) 運用中の確認

(a) 仮想ルータ状態の確認

本装置および本装置と同一仮想ルータを構成する相手装置において，仮想ルータの状態が MASTER または BACKUP になっていること，および同一仮想ルータで複数のマスタルータが存在しないことを確認してください。本装置における仮想ルータの状態確認には show vrrpstatus コマンドを使用してください。

図 6-107　仮想ルータの状態表示例

```
> show vrrpstatus
Department1:VRID 1 MASTER virtual-ip fe80::1234 priority 150
>
```

6.11.3　IEEE802.3ah/UDLD 機能の運用状態を確認する

本装置で IEEE802.3ah/UDLD 機能を使用した場合の確認内容には次のものがあります。

(1) コンフィグレーション変更後の確認

show efmoam コマンドを実行し，コンフィグレーションコマンド efmoam で定義した IEEE802.3ah/OAM 情報の設定内容が正しく反映されているかどうかを確認してください。また，本装置と接続している相手装置との間で接続確認をしたいポートについて，IEEE802.3ah/OAM に関する設定が正しいことを確認してください。

図 6-108　IEEE802.3ah/OAM の設定状態表示

(2) 運用中の確認

本装置と，本装置と接続している相手装置で show efmoam detail コマンドを実行し，以下の項目を確認してください。

- Link status が Up と表示されているポートの Dest MAC に，接続先装置の MAC アドレスが表示されていることを確認してください。
- UDLD status が active または detection と表示されているポートの Dest MAC の前に "*" が表示されていることを確認してください。

図 6-109 IEEE802.3ah/OAM の運用状態表示

```
> show efmoam detail
Date 2007/01/10 23:59:59
Status: Enabled
udld-detection-count: 30
Port   Link status    UDLD status    Dest MAC
0/1    Up             detection     *00:12:e2:98:dc:20
0/2    Down           active         unknown
0/3    Up             passive        00:12:e2:98:74:78
>
```

表示されていること。

6.12 SNMP エージェント通信の確認

6.12.1 SNMP マネージャとの通信を確認する

本装置に SNMP エージェント機能を設定して SNMP プロトコルによるネットワーク管理を行う場合，次のことを確認してください。

- ネットワーク上の SNMP マネージャから本装置に対して MIB を取得できること
- 本装置からネットワーク上の SNMP マネージャへ SNMP のトラップが送信されていること

確認手順を次に示します。なお，本装置から取得できる MIB については「MIB レファレンス　1. サポート MIB の概要」を，本装置から送信されるトラップについては「MIB レファレンス　4.2 サポートトラップ -PDU 内パラメータ」を，それぞれ参照してください。

1. ping コマンドを SNMP マネージャの IP アドレスを指定して実行し，本装置から SNMP マネージャに対して IP 通信ができることを確認してください。通信ができない場合は「8.5.1　通信ができない，または切断されている」を参照してください。
2. SNMP マネージャから本装置に対して MIB の取得ができることを確認してください。取得できない場合の対応は「8.13　SNMP の通信障害」を参照してください。

6.13 フロー統計機能の確認

6.13.1 sFlow コレクタとの通信を確認する

本装置で sFlow 統計機能を設定して sFlow コレクタに通知する場合，次のことを確認してください。

(1) sFlow コレクタとの疎通確認

ping コマンドを sFlow コレクタの IP アドレスを指定して実行し，本装置から sFlow コレクタに対して IP 通信ができることを確認してください。通信ができない場合は「8.5.1 通信ができない，または切断されている」を参照してください。

(2) sFlow パケット通信確認

sFlow コレクタ側で sFlow パケットを受信していることを確認してください。

受信していない場合の対応は「8.14 フロー統計機能の通信障害」を参照してください。

6.13.2 sFlow 統計機能を確認する

本装置で sFlow 統計機能を使用した場合，運用中の確認内容には次のものがあります。

(1) sFlow パケット廃棄の確認

show sflow コマンドを実行して sFlow 統計情報を表示し，sFlow 統計機能で破棄しているパケット数を確認してください。破棄パケット数が増加する場合は，現在のネットワークの運用状況を確認してください。

図 6-110 show sflow コマンドの実行結果

```
> show sflow
sFlow service status: enable
sFlow service version: 4
Progress time from sFlow statistics cleared: 8:00:05
Received sFlow samples:385737  Dropped sFlow samples:2093 ←── 増加していませんか？
Collector exported sFlow samples:385635  Couldn't exported sFlow samples:0
Collector IP address:192.168.4.199  UDP:6343 Source IP address:130.245.34.23
Send FlowSample UDP packets:15267  Send failed:0
（以下省略）
```

(2) CPU 使用率の確認

show cp cpu コマンドを実行して CP の CPU 使用率を表示し，負荷を確認してください。CPU 使用率が高い場合はコンフィグレーションコマンド sflow でサンプリング間隔の再設定を行ってください。

図 6-111　show cp cpu コマンドの実行結果

```
> show cp cpu minutes
*** minute ***
date    time                cpu peak   cpu average  buffer peak  buffer average
Apr 02  18:19:33-18:19:59    12           10             0             0
Apr 02  18:20:00-18:20:59    73           33             0             0
Apr 02  18:21:00-18:21:59    90           59             0             0
Apr 02  18:22:00-18:22:59    86           53             0             0
                                           ↑
                                           └── 高くありませんか？
```

6.13.3　NetFlow コレクタとの通信を確認する

本装置で NetFlow 統計機能を使用する場合，次のことを確認してください。

（1） NetFlow コレクタとの疎通確認

ping コマンドで本装置から NetFlow コレクタに対して IP 通信ができることを確認してください。通信ができない場合は「8.5.1　通信ができない，または切断されている」を参照してください。

（2） NetFlow パケット通信確認

NetFlow コレクタ側で NetFlow パケットを受信していることを確認してください。NetFlow パケットの受信の確認ついては，それぞれの NetFlow コレクタのマニュアルを参照してください。

受信していない場合の対応は「8.14　フロー統計機能の通信障害」を参照してください。

6.13.4　NetFlow 統計機能を確認する

本装置で NetFlow 統計機能を使用した場合，運用中の確認内容には次のものがあります。

（1） NetFlow 対象パケット廃棄の確認

show netflow コマンドを実行して NetFlow 統計情報を表示し，NetFlow 統計対象パケットを廃棄している数を確認してください。廃棄フロー数が増加する場合は，コンフィグレーションコマンド netflow でサンプリング間隔を調整してください。もし調整してもあふれる場合は対象のポート数を減らしてください。

図 6-112　show netflow コマンドの実行結果

```
> show netflow
Progress time from NetFlow statistics cleared: 10:00:06
PRU0: Active
  Received Flows      :     123456  Dropped Flows       :       3412  ←増加していませんか？
  Overflow Entries    :          0
  Used Entries        :       1998  Un-used Entries     :          2
Flow export Version: 5,  Service status: enable
  Active Timeout: 30 minutes,  Inactive Timeout: 15 seconds
  Collector: 10.1.1.2 udp: 6534,  Source: 10.1.1.10
    Send Flows        :        468  Discard Flows       :          0
    Send UDP Packets  :        108  Discard UDP Packets :          0
（以下省略）
```

以下の手順でサンプリング間隔を増やして,「Dropped Flows」が増加しないことを確認してください。

```
 (config)# show netflow
netflow yes
        sample 2048   ←大きな値に変更してください
        entries 0 2000
        flow-export-version 5
                destination 172.16.178.2 udp 1234
        port 1/0-2
        port 2/0
!
(config)# netflow sample 8192
(config)# show netflow
netflow yes
        sample 8192
        entries 0 2000
        flow-export-version 5
                destination 172.16.178.2 udp 1234
        port 1/0-2
        port 2/0
!
```

(2) エントリあふれの確認

show netflow コマンドを実行して NetFlow 統計情報を表示し，エントリあふれが起きていないか確認してください。エントリあふれ数が増加する場合は，関連するエントリ数を調整してください。もし調整してもあふれる場合は「Used Entries /Un-used Entries」を見て定量的に足りないようでしたら対象のポート数を減らしてください。

図 6-113　show netflow コマンドの実行結果

```
> show netflow
Progress time from NetFlow statistics cleared: 10:00:06
PRU0: Active
  Received Flows      :     123456  Dropped Flows       :       3412
  Overflow Entries    :      52430  ◀─────────────────────┐
  Used Entries        :       1998  Un-used Entries     :          2  │
Flow export Version: 5,  Service status: enable                        │
  Active Timeout: 30 minutes,  Inactive Timeout: 15 seconds            │
  Collector: 10.1.1.2 udp: 6534,  Source: 10.1.1.10                    ├── 増加していませんか？
    Send Flows        :       4468  Discard Flows       :          0  │
    Send UDP Packets  :       1608  Discard UDP Packets :          0  │
Flow Aggregation cache: protocol-port,  Service status: enable         │
  Overflow Entries    :          0  ◀─────────────────────┘
  Used Entries        :        340  Un-used Entries     :       1660
  Active Timeout: 30 minutes,  Inactive Timeout: 15 seconds
  Collector: 10.1.1.3 udp: 6534,  Source: 10.1.1.10
    Send Flows        :        428  Discard Flows       :          0
    Send UDP Packets  :        118  Discard UDP Packets :          0
（以下省略）
```

以下の手順でエントリ数を増やして，「Overflow Entries」が増加しないことを確認してください。

```
(config)# show netflow
netflow yes
        sample 2048
        entries 0 2000   ←大きな値に変更してください
        flow-export-version 5
                destination 172.16.178.2 udp 1234
        port 1/0-2
        port 2/0
!
(config)# netflow entries 0 4000
(config)# show netflow
netflow yes
        sample 2048
        entries 0 4000
        flow-export-version 5
                destination 172.16.178.2 udp 1234
        port 1/0-2
        port 2/0
!
```

(3) NetFlow パケット送信失敗の確認

show netflow コマンドを実行して NetFlow 統計情報を表示し，NetFlow パケット送信失敗数が増えていないか確認してください。NetFlow パケット送信失敗数が増加する場合は，「6.13.3　NetFlow コレクタとの通信を確認する」を参照してください。

図 6-114　show netflow コマンドの実行結果

```
> show netflow
Progress time from NetFlow statistics cleared: 10:00:06
PRU0: Active
  Received Flows      :     123456  Dropped Flows       :          0
  Overflow Entries    :          0
  Used Entries        :       1998  Un-used Entries     :          2
Flow export Version: 5,  Service status: enable
  Active Timeout: 30 minutes,  Inactive Timeout: 15 seconds
  Collector: 10.1.1.2 udp: 6534,  Source: 10.1.1.10
    Send Flows        :        468  Discard Flows       :          0
    Send UDP Packets  :        108  Discard UDP Packets :          0
Flow Aggregation cache: protocol-port,  Service status: enable
  Overflow Entries    :          0
  Used Entries        :          0  Un-used Entries     :       2000
  Active Timeout: 30 minutes,  Inactive Timeout: 15 seconds
  Collector: 10.1.1.3 udp: 6534,  Source: 10.1.1.10
    Send Flows        :        128  Discard Flows       :          0
    Send UDP Packets  :         18  Discard UDP Packets :          0
```

増加していませんか？

（4） CPU 使用率の確認

show cp cpu コマンドを実行して CP の CPU 使用率を表示し，負荷を確認してください。CPU 使用率が高い場合は，「(1) NetFlow 対象パケット廃棄の確認」「(2) エントリあふれの確認」を参照してサンプリング間隔や関連するエントリ数を調整してください。

図 6-115　show cp cpu コマンドの実行結果

```
> show cp cpu minutes
*** minute ***
date    time              cpu peak   cpu average  buffer peak  buffer average
Apr 02  18:19:33-18:19:59     0            0            0              0
Apr 02  18:20:00-18:20:59    30            3            0              0
Apr 02  18:21:00-18:21:59    90           45            0              0
Apr 02  18:22:00-18:22:59    86           59            0              0
Apr 02  18:23:00-18:23:59    36            8            0              0
```

6.14 隣接装置情報の確認

6.14.1 LLDP 機能の運用状態を確認する

本装置で LLDP 機能を使用した場合の確認内容には次のものがあります。

(1) コンフィグレーション変更後の確認

show lldp コマンドを実行し，コンフィグレーションコマンド lldp で定義した LLDP 情報の設定内容が正しく反映されているかどうかを確認してください。また，本装置と接続している相手装置との間で接続確認をしたいポートに対し，LLDP 機能に関する設定が正しいことを確認してください。

図 6-116 「LLDP の設定状態」表示例

```
> show lldp
Date 2004/04/18 10:12:26
Status: Enabled  Chassis ID: Type=MAC       Info=00:12:E2:68:2c:21
Interval Time:30   Hold Count:4  TTL:120
Port Counts=2
  0/0           Link: Up   Neighbor Counts:   1
  0/1           Link: Up   Neighbor Counts:   1
```

(2) 運用中の確認

本装置と本装置と接続している相手装置において，show lldp detail コマンドを実行し以下の項目を確認してください。

- 本装置側の表示結果で，相手装置の Chassis ID の <Info> および Port ID の <Info> が，接続しているポートの隣接装置情報として表示されていることを確認してください。
- 相手装置側の表示結果で，本装置の Chassis ID の <Info> および Port ID の <Info> が，接続しているポートの隣接装置情報として表示されていることを確認してください。

図 6-117 「LLDP の運用状態」表示例

```
> show lldp detail
Date 2004/04/18 12:26:43
Status: Enabled  Chassis ID: Type=MAC       Info=00:12:E2:68:2c:21
Interval Time: 30    Hold Count: 4  TTL: 120
System Name: LLDP1
System Description: Allied Telesis SB-7800R SB-7808R-AC [SB-7808-AC] Routing Software
SB-780S-R 9.2.B [OS-R]
Total Neighbor Counts=2
Port Counts=2
Port  0/0            Link: Up   Neighbor Counts=  1
  Port ID: Type=MAC       Info=00:12:E2:98:5c:c0
  Port Description: 10BASE-T/100BASE-TX/1000BASE-T 0/0 ether00 (lldp-test1)
  Tag ID: Untagged
  IPv4 Address: UnTagged        192.168.248.240
  IPv6 Address: Untagged        3ffe:501:811:ff01:200:8798:5cc0:e7f4
   1  TTL: 100   Chassis ID: Type=MAC      Info=00:12:E2:68:2c:2d
      System Name: LLDP2
      System Description: Allied Telesis SB-7800R SB-7808R-AC [SB-7808-AC] Routing Sof
tware SB-780S-R 9.2.B [OS-R]
      Port ID: Type=MAC       Info=00:12:E2:98:74:78
      Port Description: 10BASE-T/100BASE-TX/1000BASE-T 2/0
      Tag ID: Untagged
              Tagged=1,4095
      IPv4 Address: Untagged         192.168.248.200
      IPv6 Address: Untagged         3ffe:501:811:ff01:200:8798:7478:e7f4
Port  0/1           Link:  UP   Neighbor Counts=  1
  Port ID: Type=MAC       Info=00:12:E2:98:5c:c1
  Port Description: 10BASE-T/100BASE-TX/1000BASE-T 0/1 ether01 (lldp-test2)
  Tag ID: Untagged
  IPv4 Address: Untagged         192.168.248.250
  IPv6 Address: Untagged         3ffe:501:811:ff01:200:8798:5cc0:e7f5
  1  TTL: 110   Chassis ID: Type=MAC       Info=00:12:E2:68:25:05
     System Description: Allied Telesis SB-7800R SB-7808R-AC [SB-7808-AC] Routing Sof
tware SB-780S-R 9.2.B [OS-R]
      Port ID: Type=MAC       Info=00:12:E2:98:dc:20
      Port Description: 10BASE-T/100BASE-TX/1000BASE-T 2/0
      Tag ID: Untagged
              Tagged=1,10-20,4095
      IPv4 Address: Tagged: 10    192.168.248.220
```


6.14.2 OADP 機能の運用状態を確認する

本装置で OADP 機能を使用した場合の確認内容には次のものがあります。

(1) コンフィグレーション変更後の確認

show oadp コマンドを実行し，コンフィグレーションコマンド oadp で定義した OADP 情報の設定内容が正しく反映されているかどうかを確認してください。また，本装置と接続している相手装置との間で接続確認をしたいポートに対し，OADP 機能に関する設定が正しいことを確認してください。

図 6-118　OADP 設定および本装置 A から見た隣接情報の簡易表示例

```
> show oadp
Date 2004/02/24 23:08:25
OADP/CDP status: Enabled/Enabled    Device ID:SB-7800R-1
Interval Time: 60   Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 1/2-4

Total Neighbor Counts=2
Local     VID Holdtime Remote   VID Device ID         Capability Platform
1/2         0       35 2/1        0 SB-7800R-2        RS         SB-7800R
1/3         0       71 3/2        0 IP8800/720-1      RTS        IP8800/720
1/4         0        9 4/3        0 C2950-1           R          G2950

  Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                    S - Switch, H - Host, I - IGMP, r - Repeater
>
```

設定した値が正しいこと

（2）　運用中の確認

本装置と本装置と接続している相手装置において，show oadp detail コマンドを実行し以下の項目を確認してください。

- 本装置側に表示してある自装置の Device ID と，隣接装置側に表示してある隣接装置情報の Device ID が一致していること
- 本装置側の情報で Local と表示されているポート情報と，隣接装置側の隣接情報で Remote として表示されているポート情報が一致していること

上記項目が一致しない場合，装置間の接続が間違っている可能性がありますので接続を確認してください。

図 6-119　OADP 設定および本装置 A から見た隣接情報の詳細表示例

```
> show oadp port 1/2 detail
Date 2004/06/24 23:11:52
OADP/CDP status: Enabled/Enabled    Device ID:SB-7800R-1
Interval Time: 60   Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 1/2-4

Total Neighbor Counts=1
--------------------------------------------------------------
Port:1/2  VLAN ID: 0
  Holdtime       : 6(sec)
  Port ID        : 2/1   VLAN ID(TLV): 0
  Device ID      : SB-7800R-1
  Capabilities   : Router,Switch
  Platform       : SB-7800R
  Entry address(es):
    IP address   : 192.16.170.87
    IPv6 address: fe80::200:4cff:fe71:5d1c
  IfSpeed        : 100M   Duplex     : FULL
  Version        : Routing Software SB-780S-R 9.2.B [OS-R]

----------------------------------------------------------
```

7 運用中の作業

この章では，装置がネットワーク上で運用されている間に行う作業について説明します。

7.1 ログインユーザを追加・削除する

運用中，本装置に対して運用端末を利用するユーザが新規で発生した場合は，adduser コマンドでログインユーザを追加してください。また，利用されていないログインユーザは rmuser コマンドで削除するようにしてください。なお，登録中のログインユーザを確認する場合は，次の図に示す操作でパスワードファイル（/etc/passwd）を参照してください。

図 7-1　登録済みログインユーザの表示例

```
> cat /etc/passwd | grep tcsh
operator:*:100:100::/usr/home/operator:/bin/tcsh
user1:*:101:100::/usr/home/user1:/bin/tcsh
user2:*:102:100::/usr/home/user2:/bin/tcsh
>
```

7.2 ログインユーザのパスワードを変更する

本装置の運用中，セキュリティ強化のため定期的にログインユーザのパスワードを変更することをお勧めします。特にお勧めする契機を次に示します。

- ネットワーク構成を大幅に変更したとき
- コンフィグレーションコマンド system で本装置にログインできる運用端末 IP アドレスを新たに追加したとき
- 運用ログや運用メッセージで，不正なログインを意味するログ（「7.3.1 ログインの履歴を確認する」を参照）があったとき

なお，パスワードの変更は password コマンドを使用してください。

7.3　運用ログを確認する

7.3.1　ログインの履歴を確認する

セキュリティ強化のため，定期的に本装置へのログインの履歴を確認することをお勧めします。

(1) ログイン認証に成功したユーザを確認する

本装置へのログイン認証に成功していたユーザの履歴は”show logging | grep Login”の実行でまとめて表示できます。次の図に実行例を示します。

図 7-2　ログイン履歴の表示

```
> show logging | grep Login
EVT 07/25 12:11:20 E3 RM 00005002 1001:000000000000 Login operator from
172.16.251.69(ttyp3).
EVT 07/25 11:23:56 E3 RM 00005002 1001:000000000000 Login operator from
172.16.251.106 (ttyp2).
EVT 07/25 11:17:10 E3 RM 00005002 1001:000000000000 Login operator from
172.16.251.67(ttyp1).
(以下省略).
>
```

表示結果を基に次の観点で確認してください（ただし,”Login incorrect”が含まれているログはログイン認証失敗時に採取されるものなので，ここではチェックの対象外です)。

1. 運用端末（IP アドレス）の利用者とログインユーザ名の利用者は一致していますか。もし，一致していない場合は，運用端末の利用者にその経緯を確認してください。

(2) リモート認証に失敗したユーザを確認する

ログインを許可していないリモート運用端末からのログイン認証に失敗しているユーザの履歴は”show logging | grep ”Unknown host address””の実行でまとめて表示できます。次の図に実行例を示します。

図 7-3　ログイン履歴の表示

```
> show logging | grep "Unknown host address"
EVT 08/19 10:41:52 E3 ACCESS 00000001 0201:000000000000 Unknown host address 172
.16.251.69.
>
```

(3) ログイン認証に失敗したユーザを確認する

本装置へのログイン認証に失敗しているユーザの履歴は”show logging | grep ”Login incorrect””の実行でまとめて表示できます。次の図に実行例を示します。

図 7-4　ログイン履歴の表示

```
> show logging | grep "Login incorrect"
(途中省略)
EVT 08/01 10:38:40 E3 ACCESS 00000002 0201:000000000000 Login incorrect user2.
(以下省略)
>
```

もし履歴が多い場合，入力ミス以外の要因で採取されているのかもしれません。次のチェックを原因がわかるまで順に行ってください。

1. 「パスワードを忘れているのか」をログインユーザ名利用者全員に確認してください。忘れている利用者が存在する場合は，「8.2.3　ログインパスワードを忘れてしまった」を参照の上，対応してくださ

い。

2. 装置の管理者や同じログインユーザ名を使用するほかの利用者のパスワードが変更されていないかをshow logging コマンドで確認の上，ログインユーザ名利用者全員にパスワードの認識を徹底させてください。

図 7-5 パスワード変更履歴の検索

```
> ll /PrimaryMC/etc/passwd
-rw-r--r--  1 root  wheel  342 Aug  1 10:34 /primaryMC/etc/passwd
> show logging | grep KEY
KEY 08/01 10:35:05 user1:> show logging | grep KEY
(途中省略)
KEY 08/01 10:34:38 user2:> passwd
(以下省略)
>
```

7.3.2 障害に関するログがないかを確認する

運用中，障害に関するログが採取されていないことを定期的に確認することをお勧めします。運用中の機能すべてに影響するわけではないため発生時点では見逃される可能性のある（回線障害などのイベントレベルが低い）障害に関するログについては，特に注意してください。障害に関するログは”show logging | grep EVT”や”show logging | grep ERR”の実行でまとめて表示できます。

図 7-6 障害に関するログ表示

```
> show logging | grep EVT
(途中省略)
EVT 08/03 08:34:51 E4 LINELAN NIF:2 LINE:0 90111001 1350:02ff00000038 Error
detected on the line.
EVT 08/03 08:34:37 E4 LINELAN NIF:2 LINE:0 90110001 1350:03030000003b Line status
is up.
(以下省略)
>
```

障害に関するログの内容については「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」を参照してください。もし，show logging コマンドを実行した時点で障害が回復していない場合や頻繁に起こる障害については，「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」の［対応］や「8　トラブル発生時の対応」を参照の上，即時対応を行ってください。

7.4　SNMP トラップ情報を確認する

本装置で SNMP エージェント機能を使用すると，主に障害などが発生した場合にトラップと呼ばれるイベント通知が SNMP マネージャに送信されます。このトラップ情報によって装置の状態変化を知ることができるので，運用中は定期的に確認してください。なお，本装置固有のトラップ情報には次に示すものがあります。

表 7-1　本装置特有のトラップ情報

項番	トラップの種類	意味	発行契機
1	sb7800rSystemMsgTrap	システムメッセージ出力	システムメッセージを出力したとき。
2	sb7800rStandbySystemUpTrap	予備系 BCU 正常再起動	BCU 二重化装置で，Cold Start 以降に予備系 BCU が正常動作中であると判断したとき。
3	sb7800rStandbySystemDownTrap	予備系 BCU 異常検出	BCU 二重化装置で，Cold Start 以降に予備系 BCU が障害であると判断したとき。
4	sb7800rTemperatureTrap	温度状態の遷移	BCU の監視している温度が，正常，注意，警告，異常の各状態に遷移したとき。
5	sbrIsisAdjacencyChange	IS-IS 隣接ルータ状態変更	• IS-IS 隣接ルータの状態が変わったとき。 • IS-IS 隣接ルータが新たにできたとき。 • IS-IS 隣接ルータがなくなったとき。
6	sbrOspfVirtNbrStateChange	仮想リンクの隣接状態の遷移	仮想リンクにおいて，次に示す 1 ～ 5 の隣接状態の遷移契機で発行します。ただし，仮想リンクの Down 状態への遷移に伴う隣接 Down では発行しません。 1. Full になったとき（隣接確立） 2. ExStart 以上の状態から Down に逆行したとき 3. Full から ExStart 逆行したとき（隣接の再確立開始） 4. Full から 2way へ逆行したとき（代表ルータの変更） 5. Full から Init へ逆行したとき（隣接ルータから受信した Hello パケット内で本装置を認識しなくなったとき）
7	sbrOspfNbrStateChange	OSPF の隣接状態の遷移	仮想リンク以外のインタフェースにおいて，ospfVirtNbrStateChange と同様の隣接状態の遷移契機で発行します。ただし，OSPF インタフェースの Down 状態への遷移に伴う隣接 Down では発行しません。
8	sbrOspfVirtIfStateChange	仮想リンクのインタフェース状態の遷移	次に示す 1 ～ 2 のインタフェース状態の遷移契機で発行します。 1. 仮想リンクが Up したとき（仮想リンク上で OSPF 動作を開始） 2. 仮想リンクが Down したとき（通過エリアの障害や仮想リンクのコンフィグレーション削除等により，仮想リンク上で OSPF 動作を停止）
9	sbrOspfIfStateChange	OSPF インタフェース状態の遷移	次に示す 1 ～ 3 のインタフェース状態の遷移契機で発行します。 1. ポイント - ポイント型の OSPF インタフェースが Up したとき 2. ブロードキャスト型インタフェースにおいて，DR，Backup，DR Other 状態になったとき 3. OSPF インタフェース（仮想リンク除く）が Down したとき（物理的なダウンや，OSPF インタフェースのコンフィグレーション削除等）

項番	トラップの種類	意味	発行契機
10	sbrOspfVirtIfConfigError	仮想リンクで受信したパケットのコンフィグレーションエラー	次に示す 1 ～ 3 のエラーパケットの受信契機で発行します。 1. OSPF ヘッダのバージョン番号がバージョン 2 に指定されていない 2. 送信元がコンフィグレーションで指定された仮想ネーバでない 3. Hello パケットの場合，各パラメータ（HelloInterval, RouterDeadInterval）が一致していない
11	sbrOspfIfConfigError	OSPF インタフェースで受信したパケットのコンフィグレーションエラー	次に示す 1 ～ 3 のエラーパケットの受信契機で発行します。 1. OSPF ヘッダのバージョン番号がバージョン 2 に指定されていない 2. OSPF ヘッダのエリア ID が OSPF パケットを受信したインタフェースに定義されているエリア ID と一致しない 3. Hello パケットの場合，各パラメータ（HelloInterval, RouterDeadInterval，ネットマスク）が一致していない
12	sbrOspfVirtIfAuthFailure	仮想リンクで受信したパケットの認証エラー	仮想リンクにおいて，受信した OSPF パケットの認証方式の不一致，または認証失敗の検出契機で発行します。
13	sbrOspfIfAuthFailure	OSPF インタフェースで受信したパケットの認証エラー	仮想リンク以外のインタフェースにおいて，受信した OSPF パケットの認証方式の不一致，または認証失敗の検出契機で発行します。
14	sb7800rAirFanStopTrap	ファンが故障した	ファンの故障を検出した場合。
15	sb7800rPowerSupplyFailureTrap	電源が故障した	実装された電源のうち一つでも異常が発生した場合。
16	sb7800rLoginSuccessTrap	装置利用者がログインに成功した	ログインに成功した場合。
17	sb7800rLoginFailureTrap	装置利用者のログインが失敗した	• コンソールからのログインにおいて，1 回の認証失敗（ログイン失敗）に対して，1 回送信する。 • telnet からのログインにおいて，同一セッションで 10 回の認証に失敗し，telnet セッションを切断するときに 1 回送信する。 • access-list による切断や，login: または Password: プロンプト表示状態でのタイムアウトや強制切断時には送信しない (console で login: プロンプト出力状態での Enter キーだけの入力も送信しない)。
18	sb7800rLogoutTrap	装置利用者がログアウトした	以下の要因ログアウトが成功した場合。 • コマンド”logout”,”exit”,”quit”の場合
19	sb7800rMemoryUsageTrap	使用可能なメモリが少なくなった	使用可能なメモリが下限値を下回った場合。
20	sbrOadpNeighborCachelastChangeTrap	OADP 隣接ノードに関する情報が更新された	OADP 隣接ノードに関する情報が更新された場合。

その他のトラップ情報については，「MIB レファレンス　4.2 サポートトラップ -PDU 内パラメータ」を参照してください。

7.5 MC 容量を確認する

運用中，MC 上のファイルシステムの使用状況を show mc コマンドを用いて確認することをお勧めします。もし使用量が合計容量の 95% を超える場合は，「8.1.5 MC の容量が不足している」を参照の上，対応してください。

図 7-7 MC 容量の確認

```
> show mc
 Slot0  : primary Slot , mc-enabled
          SB-78MC256 [MC256] , SB-7800R format , 00070000
          30,866kB used (user Area: 30,866kB , dump Area: 0kB)
          200,514kB free (user Area: 175,046kB , dump Area: 25,468kB)
          231,380kB total(user Area: 205,912kB , dump Area: 25,468kB)
 Slot1  : secondary Slot , mc-enabled
          SB-78MC256 [MC256] , SB-7800R format , 00070000
          30,866kB used (user Area: 30,866kB , dump Area: 0kB)
          200,514kB free (user Area: 175,046kB , dump Area: 25,468kB)
          231,380kB total(user Area: 205,912kB , dump Area: 25,468kB)
>
```

7.6 ネットワーク構成を変更する

運用中にネットワークの構成を変更する場合，本装置では「7.6.1　ボードを追加する」～「7.6.4　コンフィグレーションを入れ替える」の作業を行ってください。

7.6.1 ボードを追加する

ネットワーク構成に収容条件がある機能を追加する場合は，PRU ／ NIF ボードの入れ替えや追加が必要になることがあります（収容条件がある機能については「解説書 Vol.1　3.2 収容条件」を参照してください）。PRU ／ NIF ボードの入れ替えや追加の操作手順は「9.4　ボード，メモリの取り外し／増設」を参照してください。

7.6.2 ランニングコンフィグレーションをバックアップする

ネットワーク構成の変更によりランニングコンフィグレーションの内容を大幅に変更する場合は，変更前と変更後のランニングコンフィグレーションをそれぞれバックアップすることをお勧めします。操作方法については「コンフィグレーションガイド　4.1 コンフィグレーションのバックアップ」を参照してください。

7.6.3 バックアップコンフィグレーションファイルを作成する

ネットワーク構成の変更によりランニングコンフィグレーションの内容を大幅に変更する場合は，事前にバックアップコンフィグレーションファイルを作成することをお勧めします。操作方法については「コンフィグレーションガイド　3.2 バックアップコンフィグレーションファイルの編集」を参照してください。

7.6.4 コンフィグレーションを入れ替える

コンフィグレーションコマンドを用いて，バックアップしたコンフィグレーションファイルを運用に使用したり，新しいネットワーク構成のコンフィグレーションファイルを運用に使用したりします。

（1） バックアップコンフィグレーションファイルを運用に使用する

copy backup-config コマンドを用いてコンフィグレーションファイルの入れ替えを運用系に対して行うと，MC のスタートアップコンフィグレーションファイルを書き替えます。書き替え後，変更後の内容で運用を開始します。なお，このとき運用中のポートが再起動するため，ネットワーク経由でログインしている場合は通信が切断されるので注意してください。

図 7-8　バックアップコンフィグレーションファイルの使用

```
> ls
backup.cnf
> enable                                               backup.cnfのコンフィグレーショ
# copy backup-config backup.cnf primary <———————       ンファイルを運用に使用
Caution: All network interface ports will be reset at command execution.
Are you sure? (y/n): y <——————— 入れ替えてもよいかどうかの確認
# quit
>
```

（2） メモリ上に記憶したランニングコンフィグレーションを待機系の運用に使用する

メモリ上に記憶したランニングコンフィグレーションを変更した場合，変更した内容はすぐに運用に反映されますが，待機系へコンフィグレーションを反映させる契機はコンフィグレーション保存 (save) を行っ

た時点で行われます。そのため，二重化運用モードが実装状態動作モード(auto_duplex)の状態で，運用系と待機系のコンフィグレーションに差分がある場合，運用系に致命的な障害が発生したり，運用系でswap bcu コマンドを実行したりすると，運用しているコンフィグレーションから入れ替わるため系切替後にすべての PRU の再起動を行い一時的に通信ができなくなります。

また，set mode コマンドで二重化運用モードを二重化固定モード(duplex)に設定している状態で，運用系と待機系のコンフィグレーションに差分がある場合，運用系での swap bcu コマンドの実行による系切替は抑止されます。また，運用系に致命的障害が発生した場合には，系切替を行わずに装置の再起動が発生します。

運用系の系切替による通信断を避け，また運用系の系切替を実行可能にするには，ランニングコンフィグレーションを変更した後にコンフィグレーションコマンド save または copy startup-config コマンドを実行し，運用系と待機系のコンフィグレーションファイルを一致させてください。

図 7-9　待機系へのコピー

7.7 系切替をする

7.7.1 実施方法

二重化運用時，運用系の BCU を交換する必要がある場合や運用系の BCU に障害がある場合は，次に示す「swap bcu コマンドによる系切替」を行ってください。ただし，BCU の障害が原因でコマンドが実行できない場合は，「BCU ALTERNATE による系切替」を行ってください（この場合，最大 30 秒間，新運用系からコマンドが実行できなくなることがあります)。

1. swap bcu コマンドによる系切替
   運用系の運用端末から swap bcu コマンドを実行すると系切替します。この場合，新待機系は再起動しません。
2. BCU ALTERNATE による系切替
   二重化で正常運用中に運用系側の BCU ボードにある BCU ALTERNATE を押すと，系切替を実行します。この場合，新待機系（BCU ALTERNATE を押した方の系）は再起動します。待機系側の BCU ALTERNATE を押しても系を切り替えません。

上記の方法で系切替ができない，または系切替をした後に PRU が再起動してしまう場合があります。「7.7.2　系切替後に PRU が再起動する要因」,「7.7.3　系切替が抑止されている要因」を参照してください。

7.7.2 系切替後に PRU が再起動する要因

本装置の二重化運用モードが実装状態動作モード (auto_duplex) で動作し，以下の状態で系切替を行うと，系切替後に PRU が再起動します。二重化がどのように運用されているかは，「運用コマンドレファレンス Vol.2　9. 二重化管理」を参照して二重化の動作モードを確認してください。

● ソフトウェアバージョンの不一致
片方の系だけ，ソフトウェアバージョンアップしている場合，この状態になります。ソフトウェアのバージョンを一致させてください。

● ソフトウェアライセンスキーの不一致
ソフトウェア購入時のソフトウェアライセンスキーが，運用系で動作している MC と待機系で動作している MC とで差分がある場合，この状態となります。ソフトウェアライセンスキーが一致した MC を使用してください。

● コンフィグレーションファイルの不一致
運用系で設定したコンフィグレーションファイルの内容が待機系に反映されていない場合，この状態になります。「5.6.2　二重化運用時の注意事項」「コンフィグレーションガイド　4.4 運用時の注意事項」を参照し，コンフィグレーションファイルを一致させてください。

7.7.3 系切替が抑止されている要因

本装置の二重化運用モードが二重化モード (duplex) で動作し以下の状態の場合，二重化運用中であっても系切替は抑止されます。二重化がどのように運用されているかは，「運用コマンドレファレンス Vol.2　9. 二重化管理」を参照して二重化の動作モードを確認してください。

● ソフトウェアバージョンの不一致
片方の系だけソフトウェアバージョンアップしている場合，この状態になります。ソフトウェアのバージョンを一致させてください。

● ソフトウェアライセンスキーの不一致
ソフトウェア購入時のソフトウェアライセンスキーが，運用系で動作している MC と待機系で動作している MC とで差分がある場合，この状態となります。ソフトウェアライセンスキーが一致した MC を使用してください。

● コンフィグレーションファイルの不一致
運用系で設定したコンフィグレーションファイルの内容が待機系に反映されていない場合，この状態になります。「5.6.2　二重化運用時の注意事項」「コンフィグレーションガイド　4.4 運用時の注意事項」を参照してコンフィグレーションファイルを一致させてください。

7.7.4　RM イーサネット運用時の注意事項

本装置の運用系と待機系の RM イーサネットは異なる MAC アドレスが設定されています。このため，運用中に系切替が発生すると，本装置の接続先 ARP テーブルまたは NDP テーブルがリフレッシュされるまでアクセスできなくなります。この場合，手動で本装置の接続先装置の ARP テーブルまたは NDP テーブルをクリアすることで，再び接続できます。また，RM イーサネットを使用してログインしているときに系切替が発生すると，コネクションが切断され，ARP テーブルまたは NDP テーブルリフレッシュ後，再度ログインするときには新運用系にログインすることになります。

7.8 ソフトウェア／コンフィグレーションを MC にバックアップする

運用中，コンフィグレーションの変更やソフトウェアのアップデートを行った場合には，その情報をバックアップ MC にコピーすることをお勧めします。次の表に，バックアップ MC にコピーするコマンドと情報を示します。

表 7-2 バックアップ MC にコピーするコマンドと情報

項番	コマンド名	バックアップ MC にコピーする情報	実行契機
1	copy mc	全情報	運用中の MC に対してソフトウェアのアップデートを行った場合
2	synchronize	次に示す情報 • ログインユーザ情報（ホームディレクトリ配下のファイル，パスワードファイル） • 冗長構成設定情報（電源ユニット，基本制御モジュール） • ランニングコンフィグレーション 詳細は運用コマンドレファレンス Vol.1 synchronize の記述を参照。	運用中の MC に対して次の操作を行った場合 • ログインユーザの追加・削除 • ログインユーザや装置管理者モードのパスワード変更 • 冗長構成設定変更 • ランニングコンフィグレーション変更
3	copy startup-config コマンドおよび copy backup-config コマンド	スタートアップコンフィグレーションファイルまたはバックアップコンフィグレーションファイル	運用中の MC に左記のファイルが新規で作成された場合

トラブル発生時の対応

本章では装置が正常に動作しない，または通信ができないといったトラブルが発生した場合の対処方法を説明します。

8.1　装置または装置の一部の障害

8.1.1　障害がシステム操作パネルに表示された

運用中，ALARM/ERROR LED が点灯し障害がシステム操作パネルに表示されたままの場合，発生した障害が回復していない状態です。この場合，以下の順で対応してください。

1. システム操作パネルの障害部位とメッセージ ID を確認してください。
2. show logging コマンドを実行して，特定した障害部位に関するログの内容を確認してください。
3. 「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」を参照して 2. で検知したログの内容を確認し，［対応］欄に明記されている対応を行ってください。

8.1.2　STATUS ランプが緑点灯以外の状態である

運用中，基本制御モジュール（BCU）の STATUS ランプが緑点灯以外の状態である場合，本装置は動作可能状態ではありません。次の表に示すとおり，STATUS ランプの状態別に対応をしてください。

表 8-1　STATUS ランプの状態と対応

STATUS ランプの状態	対応
緑点滅	本装置は起動中です。時間をおいて STATUS ランプが緑点灯になることを確認してください。
黄色点灯	本装置は二重化運用で待機系が一時的に閉塞されている状態です。待機系を運用する場合は，運用系から free standby コマンドを実行してください。
赤点灯	本装置に障害が発生して動作が停止しています。直ちに保守員に連絡してください。
消灯	電源を OFF していないでほかの LED が動作している場合，STATUS ランプの動作が不可の状態です。直ちに保守員に連絡し，その指示に従ってください。

8.1.3　系切替ができない

冗長構成の装置で系切替ができない場合は，次の表に従い確認してください。

項番	原因	確認内容
1	運用モードが一重化になっている。	show system コマンドを実行して，動作モードが duplex になっていることを確認してください。動作モードが simplex になっている場合は，系切替を実行しません。動作モードを auto_duplex または duplex に変更するには，BCU ボードが 2 枚実装されていることを確認したあと，set mode auto_duplex または set mode duplex コマンドを実行してください。
2	待機系が障害中である。	show system コマンドを実行して，待機系の状態が standby になっていることを確認してください。
3	待機系が閉塞中である。	項番 2 において，待機系の状態が close になっている場合，待機系 BCU ボードの閉塞中となっています。待機系 BCU ボードが装着されたことを確認して，運用系から free standby コマンドを実行してください。
4	動作モードが duplex で，さらに両系のコンフィグレーションが不一致である。	項番 2 において，待機系の状態が configuration discord になっている場合，copy startup-config コマンドを用いて両系のコンフィグレーションを一致させてください。なお，copy startup-config コマンド実行後，待機系は自動的に再起動します。

項番	原因	確認内容
5	動作モードがduplexで，さらに両系のソフトウェアバージョンが不一致である。	項番2において，待機系の状態がsoftware version discordになっている場合，運用系からreload stop standbyコマンドを実行して待機系をダウンさせてください。待機系のステータスLEDが黄点灯状態になったら，待機系のMCを取り外して運用系の空きMCスロットに挿入してください。その後，運用系からcopy mcコマンドを実行してください。copy mc処理が終了したら待機系にMCを戻し，待機系のリセットスイッチを押して再起動させてください。
6	動作モードがduplexで，さらに両系のソフトウェアライセンスキーが不一致である。	項番2において，待機系の状態がlicense key discordになっている場合，運用系からreload stop standbyコマンドを実行して待機系をダウンさせてください。待機系のステータスLEDが黄点灯状態になったら，待機系のMCを取り外して運用系の空きMCスロットに挿入してください。その後，運用系からcopy mcコマンドを実行してください。copy mc処理が終了したら待機系にMCを戻し，待機系のリセットスイッチを押して再起動させてください。
7	上記以外	種別ログが採取されていないかログを確認してください。種別ログが採取されている場合は，「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」を参照してメッセージごとに示されている対応を行ってください。

8.1.4 MCにアクセスできない

MCへのアクセスにトラブルが発生した場合は，次の表に従い確認をしてください。

項番	障害内容	確認内容
1	MCへの書き込みができない。	• 書き込みを行うMCが操作対象のMCスロットに正しく挿入されていること。show mcコマンドを実行して操作対象となるMCの実装状態がmc-connectであることを確認してください。 • MCの型番が正しいこと。show mcコマンドを実行して操作対象のMCの型名を確認してください。 • MCに空き容量があること。show mcコマンドを実行して操作対象のMCに空き容量が十分にあることを確認してください。
2	MCのフォーマットができない	• MCが予備側のMCスロットに正しく挿入されていること。show mcコマンドを実行して予備スロットのMCの実装状態がmc-connectであることを確認してください。 • MCの型番が正しいこと。show mcコマンドを実行してMCの型名を確認してください。

8.1.5 MCの容量が不足している

MC上のファイルシステムの使用率が100%を超えた場合に，ファイルの削除を実施して空き領域を確保しても，ファイルシステム使用率100%の状態が継続し，コンフィグレーションのセーブやファイルのコピーなどが実行できない状態となることがあります。この状態のとき，装置を停止または再起動するとMC上のファイルシステムが破壊され，MCが復旧できなくなることがあります。ファイルシステムの使用率が100%の場合またはMCの容量不足が原因でコマンドが実行できない場合は，以下の手順を実施してください。

1. 「7.5　MC容量を確認する」を参照してMCのファイルシステムの空き領域を確認してください。ファイルシステムに空き領域がない場合には，不要なファイルを削除して空き領域を確保してください。
2. ファイルの削除を実施し，空きエリアを確保してもファイルシステムの使用率が100%の状態となっている場合は，du -s /primaryMCコマンドを実行してください。本コマンドの実行により，ファイルシステム情報が更新され，MCへ書き込みができるようになります。

8.2　運用端末のトラブル

8.2.1　コンソールからの入力，表示がうまくできない

コンソールとの接続トラブルが発生した場合は，「表 8-2　コンソールとの接続トラブルおよび対応」に従い確認をしてください。

モデムとの接続トラブルが発生した場合には，「表 8-3　モデムとの接続トラブルおよび対応」に従い確認をしてください。また，モデムに付属の取扱説明書を参照してください。

表 8-2　コンソールとの接続トラブルおよび対応

項番	障害内容	確認内容
1	画面に何も表示されない	次の手順で確認してください。 1. 装置の STATUS ランプが緑点灯になっているかを確認してください。緑点灯していない場合は，「8.1.2　STATUS ランプが緑点灯以外の状態である」を参照してください。 2. ケーブルの接続が正しいか確認してください。 3. RS232C クロスケーブルを用いていることを確認してください。 4. ポート番号，通信速度，データ長，パリティビット，ストップビット，フロー制御などの通信ソフトウェアの設定が以下のとおりになっているか確認してください。 通信速度：9600bps（変更している場合は設定値） データ長：8bit パリティビット：なし ストップビット：1bit フロー制御：なし
2	キー入力を受け付けない	次の手順で確認してください。 1. XON ／ XOFF によるフロー制御でデータの送受信を中断している可能性があります。データ送受信の中断を解除してください（［Ctrl］＋［Q］をキー入力してください）。それでもキー入力ができない場合は 2. 以降の確認をしてください。 2. 通信ソフトウェアの設定が正しいか確認してください。 3. ［Ctrl］＋［S］により画面が停止している可能性があります。何かキーを入力してください。
3	ログイン時に異常な文字が表示される	通信ソフトウェアとのネゴシエーションが正しくできていない可能性があります。通信ソフトウェアの通信速度を次の手順で確認してください。 1. コンフィグレーションコマンド system で CONSOLE(RS232C) の通信速度を設定していない場合は，通信ソフトウェアの通信速度が 9600bps に設定されているか確認してください。 2. コンフィグレーションコマンド system で CONSOLE(RS232C) の通信速度を 1200，2400，4800，9600，または 19200bps に設定している場合は，通信ソフトウェアの通信速度が正しく設定されているか確認してください。 3. コンフィグレーションコマンド system で CONSOLE(RS232C) の通信速度を auto に設定している場合は，通信ソフトウェアの通信速度が 1200，2400，4800，9600，または 19200bps に設定されているか確認してください。通信ソフトウェアからブレーク信号を発行しログイン画面が表示されるか確認してください。なお，通信ソフトウェアの通信速度により複数回ブレーク信号を発行しないとログイン画面が表示されない場合があります。ブレーク信号の発行方法については，通信ソフトウェアのマニュアルを参照してください。 4. 運用端末を AUX ポートに接続している場合は，通信ソフトウェアの通信速度が 9600bps に設定されているか確認してください。
4	ユーザ名入力中に異常な文字が表示された	CONSOLE(RS232C) の通信速度を変更された可能性があります。項番 3 を参照してください。

項番	障害内容	確認内容
5	ログインできない	次のことを確認してください。 • 画面にログインプロンプトが出ていますか？　出ていなければ，装置を起動中なので，しばらくお待ちください。
6	ログイン後に通信ソフトウェアの通信速度を変更したら異常な文字が表示され，コマンド入力ができない	ログイン後に通信ソフトウェアの通信速度を変更しても正常な表示はできません。通信ソフトウェアの通信速度を元に戻してください。
7	Microsoft Windows 付属のハイパーターミナルで通信速度を変更したが通信速度が変わらない	Microsoft Windows 付属ハイパーターミナルでは，接続中に通信速度を変更しても実際の通信速度は変更されません（ステータスバーの表示は変更後の値になります)。ツールバーから切断，接続を行って通信速度を変更してください。
8	Microsoft Windows 3.1 付属のターミナルで［Ctrl］＋［C］によるコマンドの中断機能が使用できない	Microsoft Windows 3.1 付属のターミナルでは［Ctrl］＋［C］による中断機能は使用できません。
9	項目名と内容がずれて表示される	1 行で表示可能な文字数を超える情報を表示している可能性があります。通信ソフトウェアの設定で画面サイズを変更し，1 行で表示可能な文字数を多くしてください。

表 8-3　モデムとの接続トラブルおよび対応

項番	障害内容	確認内容
1	モデムが自動着信しない	次のことを確認してください。 • ケーブルの接続が正しいこと。 • モデムの電源が ON になっていること。 • 電話番号が正しいこと。 • モデムの設定内容が正しいこと。 • 2 台の端末にモデムを接続し，ダイアルすることで回線接続できること。
2	ログイン時に異常な文字が表示される	次の手順で確認してください。 1. コンフィグレーションコマンド system で CONSOLE(RS232C) の通信速度を 1200，2400，4800，または 19200bps に設定している場合は，9600bps または auto に設定してください。 2. 本装置とモデムとのネゴシエーションが正しくできていない可能性があります。コンフィグレーションで CONSOLE(RS232C) の通信速度を auto に設定している場合は，通信ソフトウェアからブレーク信号を発行しログイン画面が表示されるか確認してください。なお，複数回ブレーク信号を発行しないとログイン画面が表示されない場合があります。ブレーク信号の発行方法については，通信ソフトウェアのマニュアルを参照してください。 3. モデムが V.90, K56flex, x2 またはそれ以降の通信規格に対応している場合は，V.34 通信方式以下で接続するように設定してください。
3	何度ブレーク信号を送信しても表示が正しく行われない	ユーザがコンソールからログインしたままの状態では本装置側の接続速度を変更できません。ユーザのオートログアウトを待つか，運用端末からユーザをログアウトさせてください。
4	回線切断後，再ダイアルしても通話中でつながらない	回線切断が行われてから数秒間は着信しない場合があります。モデムのマニュアルを参照してください。

8.2.2　リモート運用端末からログインできない

リモート運用端末との接続トラブルが発生した場合は，次の表に従い確認してください。

表 8-4　リモート運用端末との接続トラブルおよび対応

項番	現象	対処方法，または参照個所
1	リモート接続ができない。	次の手順で確認してください。 1. リモート接続のための経路は確立されていますか？　PC や WS から ping コマンドを使用して経路が確立されているかを確認してください。 2. コネクション確立のメッセージ表示後プロンプトが表示されるまで時間がかかる場合は，DNS サーバとの通信ができなくなっている可能性があります（DNS サーバとの通信ができない場合プロンプトが表示されるまで約 5 分かかります。なお，この時間は目安でありネットワークの状態によって変化します）。
2	ログインができない。	次の手順で確認してください。 1. コンフィグレーションコマンド system で許可された IP または IPv6 アドレスを持つ端末を使用していますか？　また，コンフィグレーションコマンド system で設定した IP または IPv6 アドレスに restrict を指定していませんか？（詳細は「5.2.5　リモート運用端末からのログインを制限する」を参照してください） 2. ログインできる最大アカウント数を超えていませんか？（詳細は「5.2.4　同時にログインできるユーザ数を設定する」を参照してください） なお，最大アカウント数でログインしている状態でリモート運用端末から本装置への到達性が失われて，その後復旧した場合，TCP プロトコルのタイムアウト時間が経過してセッションが切断されるまで，リモート運用端末からは新たにログインできません。TCP プロトコルのタイムアウト時間はリモート運用端末の状態やネットワークの状態によって変化しますが，おおむね 10 分です。 3. コンフィグレーションコマンド system で，本装置へのアクセスを禁止しているプロトコルを使用していませんか？（詳細は「5.2.5　リモート運用端末からのログインを制限する」を参照してください）
3	キー入力を受け付けない。	次の手順で確認してください。 1. XON ／ XOFF によるフロー制御でデータの送受信を中断している可能性があります。データ送受信の中断を解除してください（［Ctrl］＋［Q］をキー入力してください）。それでもキー入力できない場合は，項番 2 以降の確認をしてください。 2. 通信ソフトウェアの設定が正しいか確認してください。 3. ［Ctrl］＋［S］により画面が停止している可能性があります。何かキーを入力してください。
4	ログインしたままの状態になっているユーザがある。	自動ログアウトするのを待つか，再度ログインしてログインしたままの状態になっているユーザを killuser コマンドで削除します。また，コンフィグレーションを編集中の場合はファイルがオープンしたままの状態になっているので，再度ログインしてクローズしてください。

8.2.3　ログインパスワードを忘れてしまった

(1)　ログインユーザのパスワード

運用中，ログインユーザのパスワードを忘れてしまい本装置にログインできない場合は，以下の手順で対応してください。

1. 装置の管理者への通知
   まずは装置の管理者に連絡してください。ただし，（ほかのログインユーザ利用者がいないなどの理由で）装置管理者モードに入るパスワードがわかるログインユーザ利用者がいない場合は，デフォルトリスタートをして再度パスワード設定を行ってください（デフォルトリスタートについての詳細は「2.2　装置を起動する」を参照してください）。
2. パスワードの変更
   パスワード変更の連絡を受けた装置の管理者は，パスワードを変更して対象ログインユーザの利用者全員に通知してください（なお，パスワードを変更する場合は password コマンドを，パスワードの削除だけ行う場合は clear password コマンドを実行してください）。

図 8-1　装置の管理者によるログインユーザパスワード変更

```
# password user1
Changing local password for user1.
New password:
New password:
#
```

（2） 装置管理者モード移行のパスワード

運用中，装置管理者モードのパスワードを知っているログインユーザ利用者全員が，パスワードを忘れてしまい装置管理者モードに入れない場合は，デフォルトリスタートをして再度パスワード設定を行ってください（デフォルトリスタートの操作方法については「2.2　装置を起動する」を参照してください）。

8.2.4　RADIUS ／ TACACS+ を利用したログイン認証ができない

RADIUS ／ TACACS+ を利用したログイン認証ができない場合，以下の確認を行ってください。

1. RADIUS ／ TACACS+ サーバへの通信
   ping コマンドで，本装置から RADIUS ／ TACACS+ サーバに対して疎通ができているかを確認してください。疎通ができない場合は，「8.5.1　通信ができない，または切断されている」を参照してください。また，コンフィグレーションでローカルアドレスを定義している場合は，ローカルアドレスから ping コマンドで，本装置から RADIUS ／ TACACS+ サーバに対して疎通ができているかを確認してください。
2. タイムアウト値およびリトライ回数設定
   RADIUS 認証の場合，コンフィグレーションコマンド radius の設定により，本装置が RADIUS サーバとの通信が不能と判断する時間は最大で＜設定したタイムアウト値（秒）＞×＜設定したリトライ回数＞×＜設定した RADIUS サーバ数＞となります。
   TACACS+ 認証の場合，コンフィグレーションコマンド tacacs+ の設定により，本装置が TACACS+ サーバとの通信が不能と判断する時間は最大で < 設定したタイムアウト値 (秒)> × < 設定した TACACS+ サーバ数＞となります。この時間が極端に大きくなると，リモート運用端末の telnet などのアプリケーションがタイムアウトによって終了する可能性があります。この場合，RADIUS ／ TACACS+ コンフィグレーションの設定かリモート運用端末で使用するアプリケーションのタイムアウトの設定を変更してください。また，運用ログに RADIUS ／ TACACS+ 認証が成功したメッセージが出力されているにもかかわらず，telnet や ftp が失敗する場合は，コンフィグレーションで指定した複数の RADIUS サーバの中で，稼働中の RADIUS ／ TACACS+ サーバに接続するまでに，リモート運用端末側のアプリケーションがタイムアウトしていることが考えられます。稼働中の RADIUS ／ TACACS+ サーバを優先するように設定するか，＜タイムアウト値（秒）＞×＜リトライ回数＞の値を小さくしてください。

8.2.5　RADIUS ／ TACACS+ を利用したコマンド承認ができない

RADIUS ／ TACACS+ 認証は成功して本装置にログインできたが，コマンド承認がうまくできない場合や，コマンドを投入しても承認エラーメッセージが表示されてコマンド実行できない場合は，以下の確認を行ってください。

1. show whoami の確認
   本装置の show whoami コマンドで，現在のユーザが許可・制限されている運用コマンドのリストを表示・確認できます。RADIUS ／ TACACS+ サーバの設定どおりにコマンドリストが取得できていることを確認してください。

2. サーバ設定の確認
   RADIUS ／ TACACS+ サーバ側で，本装置のコマンド承認に関する設定が正しいことを確認してください。特に RADIUS の場合はベンダー固有属性の設定，TACACS+ の場合は Service と属性名などに注意してください。RADIUS ／ TACACS+ サーバの設定については「5.2.6　CLI コマンドを制限する」を参照してください。
3. コマンドリスト記述時の注意
   RADIUS ／ TACACS+ サーバ側で，本装置のコマンド承認用のコマンドリストを記述する際には空白の扱いに注意してください。例えば許可コマンドリストに "show ip "（show ip の後ろにスペース）が設定してある場合は，show ip interface コマンドは許可されますが，show ipv6 interface コマンドは制限されます。

8.2.6　ローカルコマンド承認ができない

ローカル認証は成功して本装置にログインできたが，コマンド承認がうまくできない場合や，コマンドを投入しても承認エラーメッセージが表示されてコマンドが実行できない場合は，以下の確認を行ってください。

1. show whoami の確認
   本装置の show whoami コマンドで，現在のユーザが許可・制限されている運用コマンドのリストを表示・確認できます。コンフィグレーションの設定どおりにコマンドリストが設定されていることを確認してください。
2. コンフィグレーションの確認
   コンフィグレーションで，本装置のコマンド承認に関する設定が正しいことを確認してください。特にログインしたユーザ名に対応したコマンドクラスおよびコマンドリストが設定されていることを確認してください。ローカルコマンド承認の設定については「5.2.6　CLI コマンドを制限する」，「コンフィグレーションガイド　21.3 ログイン情報」，および「コンフィグレーションコマンドレファレンス Vol.2　14. ログイン情報」を参照してください。
3. コマンドリスト記述時の注意
   コンフィグレーションでコマンド承認用のコマンドリストを設定する際には空白の扱いに注意してください。例えば許可コマンドリストに "show ip "（show ip の後ろにスペース）が設定してある場合は，show ip interface コマンドは許可されますが，show ipv6 interface コマンドは制限されます。

8.3　障害情報検出

8.3.1　運用ログの中に障害に関するログが記録されている

運用ログで障害に関するログが記録されている場合，「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」を参照しながらログの内容を確認してください。

8.3.2　ダンプファイルが作成されている

ダンプファイル格納ディレクトリ（/primaryMC/var/dump）に，RM，CP，PRU，NIF のどれかのダンプファイルが採取されている場合，またはイベントダンプファイル格納ディレクトリ（/primaryMC/usr/var/evtdump/）に，イベントダンプファイルが採取されている場合は，次の作業を行ってください。なお，ダンプファイルの詳細を「表 8-5　ダンプ情報一覧」に示します。(primaryMC は現用 MC を示しています。詳細については，「解説書 Vol.2　12.6 MC」を参照してください。)

1. ファイル作成時刻を確認します
   ”show dumpfile”コマンドを実行して，ファイルが作成された時刻を確認してください。

図 8-2　ダンプファイル作成時刻の確認

```
> show dumpfile
BCU0(Active):
 MC0(Primary Slot):
  [/primaryMC/var/dump]:
    File Name              cp00.000
    Date           2005/08/03  15：52：12
    Version                SB-78OS-R 9.4
    Serial No              AA RM8MS000AR010831F001
    Error Factor   3181 80000008

  [/primaryMC/var/evtdump]:
    File Name              cpevt001.000
    Date           2005/08/03  15：52：12
    Version                SB-78OS-R 9.4
    Serial No              AA RM8MS000AR010831F001
    Error Factor   3181 80000008
```

2. ファイルが作成された要因を調査します
   show logging コマンドを実行して，ファイルが作成された時刻のログの内容を「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」を参照しながら確認してください。

図 8-3　ダンプファイル作成時のログ確認

```
> show logging
(途中省略)
EVT 08/19 16:04:04 E3 RM 00003004 1000:000000000111 RM restarted due to user
operation.
EVT 08/19 16:03:57 E3 RM 01910202 1001:000000000000 System restarted by user
operation.
(以下省略)
>
```

3. 障害情報の採取とダンプファイルの保存をします
   ダンプファイルが障害により作成されている場合は，show tech-support コマンドを実行して障害情報を採取してください（詳細は「9.1　障害情報の取得」を参照してください)。
   障害解析が必要な場合は，ダンプファイルをホームディレクトリまたは予備 MC に保存してください。
   なお，ダンプファイルをコンソールやリモート運用端末に保存する場合は，「9.2　保守情報のファイル転送」を参照してください。

4. ファイルを削除します
ファイルの保存または障害解析の終了などでダンプファイルが不要になった場合は，erase dump-file コマンドを実行して削除してください。
不要になったダンプファイルをダンプファイル格納ディレクトリに残しておくと，格納ディレクトリの空き容量不足により，ダンプ採取が正常に行われない場合があります。

表 8-5　ダンプ情報一覧

ダンプ情報	内容	格納してあるディレクトリ
CP，PRU，NIF の dump コマンドによるダンプ情報	CP，PRU，NIF のダンプ情報です。 ファイルは dump cp，dump pru，dump nif コマンドで格納します。	dump cp，dump pru，dump nif コマンドで指定したディレクトリにあります。
イベント※1により自動収集するダンプ情報	CP，PRU，NIF のイベント固有のダンプ情報です (各イベントについては「表 8-6　イベントダンプ採取イベント一覧」参照)。 ファイルは警告レベルのイベント発生時に自動で収集されます。	ダンプ情報ファイルは，/primaryMC/usr/var/evtdump/cpevt< イベント番号 >.< 収集番号 > です。 < イベント番号 > : イベント番号 (3 けた)(「表 8-6　イベントダンプ採取イベント一覧」参照) < 収集番号 > : 収集番号 (3 けた)
NIF 部障害※2時自動収集によるダンプ情報	NIF のダンプ情報です。 ファイルは NIF 部障害時に自動で収集されます。	標準のダンプ情報ファイルは，/var/dump/nif<NIF 番号 >.< 収集番号 > です (予備 MC の場合は，/secondaryMC/var/dump/nif<NIF 番号 >.< 収集番号 > です)。 <NIF 番号 > : NIF スロット番号 (2 けた) < 収集番号 > : 収集番号 (3 けた)
PRU 重度障害※3時自動収集によるダンプ情報	PRU のダンプ情報です。 ファイルは PRU 重度障害時に自動で収集されます。	標準のダンプ情報ファイルは，/var/dump/pru<PRU 番号 >.< 収集番号 > です (予備 MC の場合は，/secondaryMC/var/dump/pru<PRU 番号 >.< 収集番号 > です)。 また，拡張の PRU ダンプ情報ファイルは /secondaryMC/var/dump/pru<PRU 番号 >e1.< 収集番号 > です。 <PRU 番号 > : PRU スロット番号 (2 けた) < 収集番号 > : 収集番号 (3 けた)
CP 重度障害※4時自動収集によるダンプ情報	CP のダンプ情報です。 ファイルは CP 重度障害時に自動で収集されます。	ダンプ情報ファイルは，/var/dump/cp00.< 収集番号 > です (予備 MC の場合は，/secondaryMC/var/dump/cp00.< 収集番号 > です)。 また，拡張の CP ダンプ情報ファイルは /secondaryMC/var/dump/cp00e1.< 収集番号 > です。 < 収集番号 > : 収集番号 (3 けた)
致命的障害※5時自動収集によるダンプ情報	RM のダンプ情報です。 ファイルは致命的障害時に自動で収集されます。	ダンプ情報ファイルは，/var/dump/rmdump です (予備 MC の場合は，/secondaryMC/var/dump/rmdump です)。

注※1　イベントは種別ログのイベントレベルが E3 ～ E4（詳細は「メッセージ・ログレファレンス　1.4 ログの確認」を参照）を示しています。
注※2　NIF 部障害は種別ログのイベントレベルが E6（詳細は「メッセージ・ログレファレンス　1.4 ログの確認」を参照）を示しています。
注※3　PRU 重度障害は種別ログのイベントレベルが E8（詳細は「メッセージ・ログレファレンス　1.4 ログの確認」を参照）を示しています。
注※4　CP 重度障害は種別ログのイベントレベルが E8（詳細は「メッセージ・ログレファレンス　1.4 ログの確認」を参照）を示しています。
注※5　致命的障害は種別ログのイベントレベルが E9（詳細は「メッセージ・ログレファレンス　1.4 ログの確認」を参照）を示しています。

表 8-6　イベントダンプ採取イベント一覧

イベント番号	イベント内容	情報採取契機	ファイル作成契機	イベントレベル	イベント発生部位	メッセージ識別	付加情報	メッセージテキスト
001	CP 輻輳	CP 輻輳メッセージ出力から CP 輻輳回復メッセージが出力されるまで。ただしファイル作成後から 10 分間は情報採取しない。	CP 輻輳回復メッセージ出力後。または，CP 輻輳状態が 5 分間続いた場合。	E4	CP	80000003	1132	Congestion detected on CP.
				E4	CP	80000004	1134	CP recovered from congestion.

8.3.3　コアファイルが作成されている

コアファイル格納ディレクトリ（/primaryMC/var/core）にコアファイルが作成されている場合は，次の作業を行ってください。

1. ファイル作成時刻を確認します
   ” ls -l”を実行して，ファイルが作成された時刻を確認してください。

図 8-4　コアファイル作成時刻の確認

```
> ls -l /primaryMC/var/core
-rwxrwxrwx  1 root  wheel  1153219 Jun 21 16:35 rtm.core
>
```

2. ファイルが作成された要因を調査します
   show logging コマンドを実行して，ファイルが作成された時刻のログの内容を「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」を参照しながら確認してください。

図 8-5　コアファイル作成時のログ確認

```
> show logging
(途中省略)
EVT 06/21 16:36:27 R7 RM 05001001 1001:000000000000 rtm restarted.
(以下省略)
>
```

3. 障害情報を採取します
   コアファイルが障害により作成されている場合は，show tech-support コマンドを実行して障害情報を採取してください（詳細は「9.1　障害情報の取得」を参照してください）。
4. ファイルを保存します
   障害解析などで必要な場合は，コアファイルを保存してください。なお，コアファイルをコンソールやリモート運用端末に保存する場合は「9.2　保守情報のファイル転送」を参照してください。また，予備 MC に保存する場合は cp コマンドを実行してください。
5. ファイルを削除します
   障害解析の終了などでコアファイルが不要になった場合は，rm コマンドを実行して削除してください。

8.4　ネットワークインタフェースの通信障害

8.4.1　イーサネット回線の接続ができない

通信障害の原因がイーサネット回線にあると考えられる場合は，NIF，Line の各状態を以下に従い確認してください。

（1） NIF の状態確認

show interfaces コマンドにより NIF 状態を確認してください。次の表に NIF 状態に対する対応を示します。

表 8-7　NIF 状態の確認および対応

項番	NIF 状態	原因	対応
1	active	当該 NIF は正常に動作中です。	「表 8-8　Line 状態の確認および対応」により Line の状態を確認してください。
2	mismatch	実装されている NIF と Line コンフィグレーションが不一致です。	実装している NIF が間違っていないか，または Line のコンフィグレーションが間違っていないか確認してください。
		当該 NIF に以下が実装され，system コンフィグレーションに 16k インタフェースモードが設定されているため，コンフィグレーションが不一致となっています。 • NE1G-48T	左記の NIF を使用する場合は system コンフィグレーションの interface_mode パラメータを 8k インタフェースモードに設定してください。設定後，運用可能となります。インタフェースモードの設定方法については，「コンフィグレーションガイド　5.1.1 NE1G-48T を実装する」を参照してください。または実装すべき NIF が間違っている場合は NIF を交換してください。
3	unused	当該 NIF が実装されていません。	NIF ボードを実装し，free コマンドにより当該 NIF を運用状態にしてください。
4	closed	close コマンドにより当該 NIF が閉塞されています。	使用する NIF ボードが実装され，本ソフトウェアバージョンでサポートされていることを確認の上，free コマンドにより当該 NIF を運用状態にしてください。
5	fault	当該 NIF が障害となっています。	show logging コマンドにより表示される当該 Line のログより，「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」の該当個所を参照し，記載されている［対応］に従って対応してください。
6	initialize	当該 NIF が障害検出後の再起動中です。	同上
7	locked	コンフィグレーションにより当該 NIF が閉塞されています。	使用する NIF ボードが実装されていることを確認の上，コンフィグレーションを設定して当該 NIF を運用状態にしてください。

（2） Line の状態確認

show interfaces コマンドにより Line 状態を確認してください。次の表に Line 状態に対する対応を示します。

表 8-8　Line 状態の確認および対応

項番	Line 状態	原因	対応
1	active up	当該回線は正常に動作中です。	なし

項番	Line 状態	原因	対応
2	active down	当該 Line に回線障害が発生しています。	show logging コマンドにより表示される当該 Line のログより，「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」の該当個所を参照し，記載されている［対応］に従って対応してください。
3	unused	当該回線に Line コンフィグレーションが設定されていません。	使用する回線の Line コンフィグレーションを設定してください。
4	closed	close コマンドにより当該回線が閉塞されています。	使用する回線にケーブルが接続されていることを確認の上，free コマンドにより当該 Line を運用状態にしてください。
5	test	test interfaces コマンドにより，当該回線は回線テスト中です。	通信を再開する場合は，no test interfaces コマンドにより回線テストを停止してください。
6	fault	当該回線の回線部分のハードウェアが障害となっています。	show logging コマンドにより表示される当該回線のログより，「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」の該当個所を参照し，記載されている［対応］に従って対応してください。
7	initialize	当該回線が障害検出後の再起動中です。	同上
8	locked	コンフィグレーションにより当該回線が閉塞されています。	使用する回線にケーブルが接続されていることを確認の上，コンフィグレーションを設定して当該回線を運用状態にしてください。

8.4.2 10BASE-T/100BASE-TX/1000BASE-T のトラブル発生時の対応

10BASE-T/100BASE-TX/1000BASE-T でトラブルが発生した場合は，以下の順序で障害の切り分けを行ってください。

1. ログの確認
   ログは「メッセージ・ログレファレンス　3.5.1 イベント発生部位＝ LINELAN」および「メッセージ・ログレファレンス　3.9 ネットワークインタフェースモジュール・イーサネット」を参照してください。
2. 障害解析方法に従った原因の切り分け
   以下の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 8-9　10BASE-T/100BASE-TX/1000BASE-T のトラブル発生時の障害解析方法

項番	確認内容	原因	対応
1	show interfaces コマンドの障害統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • Link down	回線品質が低下しています。	ケーブルがカテゴリ 5 以上で 8 芯 4 対か確認してください。
			ピンマッピングが MDI となっているか確認してください。
			ケーブル長を確認してください。ケーブル長は「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。

項番	確認内容	原因	対応
			本装置でサポートしている接続インタフェースに交換してください。本装置でサポートしている接続インタフェースは「解説書 Vol.1　4.2.1 10BASE-T ／ 100BASE-TX ／ 1000BASE-T」を参照してください。
			相手装置の送信側機能に問題ないか確認してください。相手装置に回線テスト機能がある場合，相手装置の回線テストを実行してください。
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。no test interfaces（イーサネット）コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「9.7　回線をテストする」を参照してください。
2	show interfaces コマンドの受信系エラー統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • CRC errors • Layer 1 symbol errors • Layer 2 symbol errors		ケーブルがカテゴリ 5 以上で 8 芯 4 対か確認してください。
			ピンマッピングが MDI となっているか確認してください。
			ケーブル長を確認してください。ケーブル長は「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。
			本装置でサポートしている接続インタフェースに交換してください。本装置でサポートしている接続インタフェースは「解説書 Vol.1　4.2.1 10BASE-T ／ 100BASE-TX ／ 1000BASE-T」を参照してください。
			相手装置の送信側機能に問題ないか確認してください。相手装置に回線テスト機能がある場合，相手装置の回線テストを実行してください。
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。「運用コマンドレファレンス Vol.1　no test interfaces（イーサネット）」の実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「9.7　回線をテストする」を参照してください。
3	show interfaces コマンドの障害統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • Down shift	ケーブルがカテゴリ 5 以上で 8 芯 4 対ではありません。	カテゴリ 5 以上で 8 芯 4 対のケーブルと交換してください。
		ケーブルのピンマッピングが不正です。	ピンマッピングを正しく直してください。ピンマッピングは「解説書 Vol.1　4.2.1 10BASE-T ／ 100BASE-TX ／ 1000BASE-T」を参照してください。
4	show interfaces コマンドの障害統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • MDI cross over changed	ケーブルのピンマッピングが不正です。	ピンマッピングを正しく直してください。ピンマッピングは「解説書 Vol.1　4.2.1 10BASE-T ／ 100BASE-TX ／ 1000BASE-T」を参照してください。

項番	確認内容	原因	対応
5	show interfaces コマンドの Line detail 情報により該当回線で Line 種別 / 回線速度を確認してください。不正な Line 種別 / 回線速度の場合，原因と対応欄を参照してください。	カテゴリ 5 以上で 8 芯 4 対ではありません。	カテゴリ 5 以上で 8 芯 4 対のケーブルと交換してください。
		コンフィグレーションコマンド line の type が相手装置と不一致です。	コンフィグレーションコマンド line の type を相手装置と合わせてください。

8.4.3　1000BASE-X のトラブル発生時の対応

1000BASE-X でトラブルが発生した場合は，以下の順序で障害の切り分けを行ってください。

1. ログの確認
   ログは「メッセージ・ログレファレンス　3.5.1 イベント発生部位＝ LINELAN」および「メッセージ・ログレファレンス　3.9 ネットワークインタフェースモジュール・イーサネット」を参照してください。
2. 障害解析方法に従った原因の切り分け
   以下の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 8-10　1000BASE-X のトラブル発生時の障害解析方法

項番	確認内容	原因	対応
1	show interfaces コマンドの障害統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • Link down • Signal detect errors	受信側の回線品質が低下しています。	光ファイバの種別を確認してください。モードは「解説書 Vol.1　4.2.2 1000BASE-X」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「解説書 Vol.1　4.2.2 1000BASE-X」を参照してください。
			ケーブル長を確認してください。ケーブル長は「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合，汚れをふき取ってください。
			トランシーバの接続が正しいか確認してください。
			コンフィグレーションコマンド line の type を相手装置と合わせてください。
			相手装置のトランシーバのセグメント規格（SX/LX/LH）と合わせてください。
			光レベルが正しいか確認してください。光レベルは「解説書 Vol.1　4.2.2 1000BASE-X」を参照してください。
			相手装置の送信側機能に問題ないか確認してください。相手装置に回線テスト機能がある場合，相手装置の回線テストを実行してください。

項番	確認内容	原因	対応
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。no test interfaces（イーサネット）コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「9.7　回線をテストする」を参照してください。
2	show interfaces コマンドの受信系エラー統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • CRC errors • Layer 1 symbol errors • Layer 2 symbol errors		光ファイバの種別を確認してください。モードは「解説書 Vol.1　4.2.2 1000BASE-X」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「解説書 Vol.1　4.2.2 1000BASE-X」を参照してください。
			ケーブル長を確認してください。ケーブル長は「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合，汚れをふき取ってください。
			トランシーバの接続が正しいか確認してください。
			コンフィグレーションコマンド line の type を相手装置と合わせてください。
			相手装置のトランシーバのセグメント規格（SX/LX/LH）と合わせてください。
			光レベルが正しいか確認してください。光レベルは「解説書 Vol.1　4.2.2 1000BASE-X」を参照してください。
			相手装置の送信側機能に問題ないか確認してください。相手装置に回線テスト機能がある場合，相手装置の回線テストを実行してください。
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。「運用コマンドレファレンス Vol.1　no test interfaces（イーサネット）」の実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「9.7　回線をテストする」を参照してください。
3	show interfaces コマンドの障害統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • TX fault	トランシーバが故障しています。	トランシーバを交換してください。

8.4.4　10GBASE-R および 10GBASE-W のトラブル発生時の対応

10GBASE-R および 10GBASE-W でトラブルが発生した場合は，以下の順序で障害の切り分けを行ってください。

1. ログの確認
   ログは「メッセージ・ログレファレンス　3.5.1 イベント発生部位＝ LINELAN」および「メッセージ・ログレファレンス　3.9 ネットワークインタフェースモジュール・イーサネット」を参照してください。
2. 障害解析方法に従った原因の切り分け
   以下の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 8-11　10GBASE-R および 10GBASE-W のトラブル発生時の障害解析方法

項番	確認内容	原因	対応
1	show interfaces コマンドの障害統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • Signal detect errors • LOS of sync • HI_BER • LF	受信側の回線品質が低下しています。	光ファイバの種別を確認してください。モードは「解説書 Vol.1　4.2.3 10 ギガビット・イーサネット (10GBASE-R)」または「解説書 Vol.1　4.2.4 10 ギガビット・イーサネット WAN(10GBASE-W)」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「解説書 Vol.1　4.2.3 10 ギガビット・イーサネット (10GBASE-R)」または「解説書 Vol.1　4.2.4 10 ギガビット・イーサネット WAN(10GBASE-W)」を参照してください。
			ケーブル長を確認してください。ケーブル長は「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合，汚れをふき取ってください。
			トランシーバを交換可能な NIF の場合，トランシーバの接続が正しいか確認してください。
			トランシーバを交換可能な NIF の場合，相手装置のトランシーバのセグメント規格 (LR) と合わせてください。
			光レベルが正しいか確認してください。光レベルは「解説書 Vol.1　4.2.3 10 ギガビット・イーサネット (10GBASE-R)」または「解説書 Vol.1　4.2.4 10 ギガビット・イーサネット WAN(10GBASE-W)」を参照してください。
			相手装置の送信側機能に問題ないか確認してください。相手装置に回線テスト機能がある場合，相手装置の回線テストを実行してください。
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。no test interfaces（イーサネット）コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「9.7　回線をテストする」を参照してください。

項番	確認内容	原因	対応
2	show interfaces コマンドの受信系エラー統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • CRC errors • Symbol errors		光ファイバの種別を確認してください。モードは「解説書 Vol.1　4.2.3 10 ギガビット・イーサネット (10GBASE-R)」または「解説書 Vol.1　4.2.4 10 ギガビット・イーサネット WAN(10GBASE-W)」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「解説書 Vol.1　4.2.3 10 ギガビット・イーサネット (10GBASE-R)」または「解説書 Vol.1　4.2.4 10 ギガビット・イーサネット WAN(10GBASE-W)」を参照してください。
			ケーブル長を確認してください。ケーブル長は「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合，汚れをふき取ってください。
			トランシーバを交換可能な NIF の場合，トランシーバの接続が正しいか確認してください。
			トランシーバを交換可能な NIF の場合，相手装置のトランシーバのセグメント規格 (LR) と合わせてください。
			光レベルが正しいか確認してください。光レベルは「解説書 Vol.1　4.2.3 10 ギガビット・イーサネット (10GBASE-R)」または「解説書 Vol.1　4.2.4 10 ギガビット・イーサネット WAN(10GBASE-W)」を参照してください。
			相手装置の送信側機能に問題ないか確認してください。相手装置に回線テスト機能がある場合，相手装置の回線テストを実行してください。
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。「運用コマンドレファレンス Vol.1　no test interfaces（イーサネット）」の実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「9.7　回線をテストする」を参照してください。
3	show interfaces コマンドの障害統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • RF	送信側の回線品質が低下しています。	光ファイバの種別を確認してください。モードは「解説書 Vol.1　4.2.3 10 ギガビット・イーサネット (10GBASE-R)」または「解説書 Vol.1　4.2.4 10 ギガビット・イーサネット WAN(10GBASE-W)」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「解説書 Vol.1　4.2.3 10 ギガビット・イーサネット (10GBASE-R)」または「解説書 Vol.1　4.2.4 10 ギガビット・イーサネット WAN(10GBASE-W)」を参照してください。
			ケーブル長を確認してください。ケーブル長は「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合，汚れをふき取ってください。

項番	確認内容	原因	対応
			トランシーバを交換可能な NIF の場合，トランシーバの接続が正しいか確認してください。
			トランシーバを交換可能な NIF の場合，相手装置のトランシーバのセグメント規格 (LR) と合わせてください。
			光レベルが正しいか確認してください。光レベルは「解説書 Vol.1　4.2.3 10 ギガビット・イーサネット (10GBASE-R)」または「解説書 Vol.1　4.2.4 10 ギガビット・イーサネット WAN(10GBASE-W)」を参照してください。
			相手装置の受信側機能に問題ないか確認してください。相手装置に回線テスト機能がある場合，相手装置の回線テストを実行してください。
			本装置の回線テストを実行して送信側機能に問題ないか確認してください。no test interfaces（イーサネット）コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「9.7　回線をテストする」を参照してください。

8.4.5　10GBASE-W での SONET/SDH 装置との接続ができない

本装置と SONET/SDH 装置との接続ができない場合は，ログを確認してください。次の表に示す障害解析方法に従って原因の切り分けを行ってください。ログは「メッセージ・ログレファレンス　3.5.1 イベント発生部位＝ LINELAN」および「メッセージ・ログレファレンス　3.9 ネットワークインタフェースモジュール・イーサネット」を参照してください。

表 8-12　SONET/SDH 装置との接続ができない場合の障害解析方法

項番	確認内容	原因	対応
1	show interfaces コマンドの障害統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • LOS • LOF • B2SD • P-LOP • P-LCD • S-BIP8 • L-BIP1536 • P-BIP8	回線クロックの同期がとれていません。	コンフィグレーションコマンド line の clock と相手装置の同期クロックの設定が正しい組み合わせか確認してください。本装置のクロックを external に設定している場合，相手装置のクロックを independent に設定してください。本装置のクロックを external に設定し，相手装置を SONET/SDH 装置とする場合，相手装置の入力周波数精度を確認してください。入力周波数精度は，「解説書 Vol.1　4.2.4(5) クロック」を参照してください。
		受信側の回線品質が低下しています。	光ファイバの種別を確認してください。モードは「解説書 Vol.1　4.2.4 10 ギガビット・イーサネット WAN(10GBASE-W)」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「解説書 Vol.1　4.2.4 10 ギガビット・イーサネット WAN(10GBASE-W)」を参照してください。
			ケーブル長を確認してください。ケーブル長は「ハードウェア取扱説明書」を参照してください。

項番	確認内容	原因	対応
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合，汚れをふき取ってください。
			光レベルが正しいか確認してください。光レベルは「解説書 Vol.1　4.2.4 10 ギガビット・イーサネット WAN(10GBASE-W)」を参照してください。
			相手装置の送信側機能に問題ないか確認してください。相手装置に回線テスト機能がある場合，相手装置の回線テストを実行してください。
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。no test interfaces（イーサネット）コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「9.7　回線をテストする」を参照してください。
2	show interfaces コマンドの障害統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • L-RDI • P-RDI • RDI P-AIS/P-LOP • L-REI • P-REI	回線クロックの同期がとれていません。	コンフィグレーションコマンド line の clock と相手装置の同期クロックの設定が正しい組み合わせか確認してください。本装置のクロックを external に設定している場合，相手装置のクロックを independent に設定してください。本装置のクロックを external に設定し，相手装置を SONET/SDH 装置とする場合，相手装置の入力周波数精度を確認してください。入力周波数精度は，「解説書 Vol.1　4.2.4(5) クロック」を参照してください。
		送信側の回線品質が低下しています。	光ファイバの種別を確認してください。モードは「解説書 Vol.1　4.2.4 10 ギガビット・イーサネット WAN(10GBASE-W)」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「解説書 Vol.1　4.2.4 10 ギガビット・イーサネット WAN(10GBASE-W)」を参照してください。
			ケーブル長を確認してください。ケーブル長は「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合，汚れをふき取ってください。
			光レベルが正しいか確認してください。光レベルは「解説書 Vol.1　4.2.4 10 ギガビット・イーサネット WAN(10GBASE-W)」を参照してください。
			相手装置の受信側機能に問題ないか確認してください。相手装置に回線テスト機能がある場合，相手装置の回線テストを実行してください。
			本装置の回線テストを実行して送信側機能に問題ないか確認してください。no test interfaces（イーサネット）コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「9.7　回線をテストする」を参照してください。

項番	確認内容	原因	対応
3	show interfaces コマンドの障害統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • RDI P-PLM/P-LCD	RDI モード設定が相手装置と不一致です。	コンフィグレーションコマンド line の rdi と相手装置の RDI モードの設定が一致しているか確認してください。不一致の場合，一致するように設定してください。
		C2 の設定が相手装置と不一致です。	コンフィグレーションコマンド line の c2 と相手装置の C2 の設定が一致しているか確認してください。不一致の場合，一致するように設定してください。
		送信側の回線品質が低下しています。	光ファイバの種別を確認してください。モードは「解説書 Vol.1　4.2.4 10 ギガビット・イーサネット WAN(10GBASE-W)」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「解説書 Vol.1　4.2.4 10 ギガビット・イーサネット WAN(10GBASE-W)」を参照してください。
			ケーブル長を確認してください。ケーブル長は「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合，汚れをふき取ってください。
			光レベルが正しいか確認してください。光レベルは「解説書 Vol.1　4.2.4 10 ギガビット・イーサネット WAN(10GBASE-W)」を参照してください。
			相手装置の受信側機能に問題ないか確認してください。相手装置に回線テスト機能がある場合，相手装置の回線テストを実行してください。
			本装置の回線テストを実行して送信側機能に問題ないか確認してください。no test interfaces（イーサネット）コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「9.7　回線をテストする」を参照してください。
4	show interfaces コマンドの障害統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • P-PLM	C2 の設定が相手装置と不一致です。	コンフィグレーションコマンド line の c2 と相手装置の C2 の設定が一致しているか確認してください。不一致の場合，一致するように設定してください。
5	show interfaces コマンドの Line detail 情報により該当回線で以下の値が一致しているか確認してください。不一致の場合，原因と対応欄を参照してください。 • section trace message send と section trace message receive	セクショントレースメッセージが相手装置と不一致です。※	コンフィグレーションコマンド line の section_trace_message_mode と相手装置のセクショントレースメッセージの設定が一致しているか確認してください。不一致の場合，一致するように設定してください。
			コンフィグレーションコマンド line の j0 と相手装置の J0 の設定が一致しているか確認してください。不一致の場合，一致するように設定してください。

項番	確認内容	原因	対応
6	show interfaces コマンドの Line detail 情報により該当回線で以下の値が一致しているか確認してください。不一致の場合，原因と対応欄を参照してください。 • path trace message send と path trace message receive	パストレースメッセージが相手装置と不一致です。	コンフィグレーションコマンド line の path_trace_message_mode と相手装置のパストレースメッセージの設定が一致しているか確認してください。不一致の場合，一致するように設定してください。
			コンフィグレーションコマンド line の j1 と相手装置の J1 の設定が一致しているか確認してください。不一致の場合，一致するように設定してください。
7	コンフィグレーションコマンド line の ss と相手装置の SS ビットの設定が一致しているか確認してください。不一致の場合，原因と対応欄を参照してください。	SS ビットが相手装置と不一致です。※	コンフィグレーションコマンド line の ss と相手装置の SS ビットの設定が一致しているか確認してください。不一致の場合，一致するように設定してください。

注※　本装置は不一致の場合でも回線障害とせずに正常に動作します。相手装置が不一致の場合に回線障害とする装置であると接続できません。

8.4.6　リンクアグリゲーション使用時の通信障害

リンクアグリゲーション使用時に通信ができない，または縮退運転している場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 8-13　リンクアグリゲーション使用時の通信の障害解析方法

項番	確認内容・コマンド	対応
1	通信障害となっているリンクアグリゲーションの設定を show link-aggregation コマンドで確認してください。	リンクアグリゲーションのモードが相手装置のモードと同じ設定になっているか確認してください。相手装置とモードが異なった場合，相手装置と同じモードに変更してください。
		リンクアグリゲーションのモードが一致している場合 • LACP 開始方法が両方とも passive になっていないか確認してください。両方とも passive になっていた場合，どちらか一方を active に変更してください。 • Actor 装置の Key が正しく設定されていることを確認してください。
2	通信障害となっているポートの運用状態を show link-aggregation detail コマンドで確認してください。	各ポートの状態（Status）を確認してください。リンクアグリゲーショングループ内の全ポートが Down の場合，リンクアグリゲーションのグループが Down します。 Down ポートは Reason の表示によって以下を行ってください。 • LA Disabled リンクアグリゲーショングループが Disable 状態となって DOWN しています。 • Port Down リンクダウンしています。「8.4　ネットワークインタフェースの通信障害」を参照してください。 • Port Speed Unmatch リンクアグリゲーショングループ内の他ポートと回線速度が不一致となって縮退状態になっています。縮退を回避する場合はリンクアグリゲーショングループ内の全ポートの速度が一致するようにしてください。

項番	確認内容・コマンド	対応
		• Duplex Half モードが Half となって縮退状態になっています。縮退を回避する場合は Duplex モードを Full に設定してください。 • Port Selecting ポートアグリゲーション条件チェック実施中のため，縮退状態になっています。チェックが終了するまでしばらくお待ちください。 • Waiting Partner Synchronization ポートアグリゲーション条件チェックを完了し接続ポートの同期待ちとなって縮退状態になっています。しばらく待っても回復しない場合は相手装置の運用状態の確認，および設定の確認をしてください。 • Partner System ID Unmatch 接続ポートから受信した Partner System ID がグループの Partner System ID と不一致となって縮退状態になっています。縮退を回避する場合は相手装置の運用状態の確認，配線の確認をしてください。 • LACPDU Expired 接続ポートからの LACPDU 有効時刻を超過したため，該当ポートが縮退状態となっています。show link-aggregation statistics lacp コマンドで LACPDU の統計情報を確認してください。また相手装置の運用状態の確認をしてください。
		• Partner Key Unmatch 接続ポートから受信した Key がグループの Partner Key が不一致のため縮退状態となっています。縮退を回避する場合は相手装置の運用状態の確認，配線の確認をしてください。 • Partner Aggregation Individual 接続ポートからリンクアグリゲーション不可を受信したため縮退状態となっています。縮退を回避する場合は相手装置の運用状態の確認，および設定の確認をしてください。 • Partner Synchronization OUT_OF_SYNC 接続ポートから同期不可を受信したため縮退状態となっています（本装置でコンフィグレーションを変更した場合や相手装置で回線の閉塞を行った場合に発生します）。 • Port Moved 接続されていたポートが他のポートと接続しました。配線の確認をしてください。 • Actor key Unspecified 本装置で Key が設定されていないため縮退状態となっています。Key を設定してください。 • Operation of Detach Port Limit 離脱ポート数制限機能が動作したため，リンクアグリゲーショングループが Down しています。

8.4.7 POS 回線の接続ができない

通信障害の原因が POS 回線にあると考えられる場合は，NIF，Line，PPP の各状態を以下に従い確認してください。

(1) NIF の状態確認

show interfaces コマンドにより NIF 状態を確認してください。NIF 状態に対する対応を次の表に示します。

表 8-14　NIF 状態の確認および対応

項番	NIF 状態	原因	対応
1	active	当該 NIF は正常に動作中です。	「表 8-15　Line 状態の確認および対応」により Line 状態を確認してください。
2	mismatch	実装されている NIF と Line コンフィグレーションが不一致です。	実装している NIF が間違っていないか，または Line コンフィグレーションが間違っていないか確認してください。
3	unused	当該 NIF が実装されていません。	NIF ボードを実装し，free コマンドにより当該 NIF を運用状態にしてください。
4	closed	当該 NIF が閉塞されています。	使用する NIF ボードが実装され，本ソフトウェアバージョンでサポートされていることを確認のうえ，free コマンドにより当該 NIF を運用状態にしてください。
5	fault	当該 NIF が障害となっています。	show logging コマンドにより表示される当該 Line のログより，「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」の該当個所を参照し，記載されている［対応］に従って対応してください。
6	initialize	当該 NIF が障害検出後の再起動中です。	同上
7	locked	コンフィグレーションにより当該 NIF が閉塞されています。	使用する NIF ボードが実装されていることを確認のうえ，コンフィグレーションを設定して当該 NIF を運用状態にしてください。

（2） Line の状態確認

show interfaces コマンドにより Line 状態を確認してください。Line 状態に対する対応を次の表に示します。

表 8-15　Line 状態の確認および対応

項番	Line 状態	原因	対応
1	active up	当該回線は正常に動作中です。	なし
2	active down	当該回線に回線障害が発生しています。	show logging コマンドにより表示される当該 Line のログより，「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」の該当個所を参照し，記載されている［対応］に従って対応してください。
3	unused	当該回線に Line コンフィグレーションが設定されていません。	使用する回線の Line コンフィグレーションを設定してください。
4	closed	当該 Line が閉塞されています。	使用する Line にケーブルが接続されていることを確認のうえ，free コマンドにより当該 Line を運用状態にしてください。
5	test	test interfaces コマンドにより，当該 Line は回線テスト中です。	通信を再開する場合は，no test interfaces コマンドにより回線テストを停止してください。
6	fault	当該 Line の回線部分のハードウェアが障害となっています。	show logging コマンドにより表示される当該 Line のログより，「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」の該当個所を参照し，記載されている［対応］に従って対応してください。
7	initialize	当該 Line が障害検出後の再起動中です。	同上

項番	Line 状態	原因	対応
8	locked	コンフィグレーションにより当該 Line が閉塞されています。	使用する Line にケーブルが接続されていることを確認のうえ，コンフィグレーションを設定して当該 Line を運用状態にしてください。

（3） PPP 状態の確認

show interfaces コマンドにより PPP の LCP，各 NCP の状態を確認してください。PPP 状態に対する対応を次の表に示します。

表 8-16　PPP 状態の確認および対応

項番	PPP 状態	原因	対応
1	LCP 状態が up である	相手装置との間で LCP が確立しています。	対象の NCP 状態を確認してください。
2	LCP 状態が down である	相手装置との間で LCP が確立していません。	show logging コマンドにより表示される該当 Line のログより，「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」の該当個所を参照し，記載されている［対応］に従って対応してください。
3	IPCP 状態が up である	相手装置との間で IPCP が確立しています。	「8.5　IPv4 ネットワークの通信障害」を参照してください。
4	IPCP 状態が down である	相手装置との間で IPCP が確立していません。	IP アドレスコンフィグレーションが設定されているか確認してください。上記以外の場合は show logging コマンドにより表示される該当 Line のログより，「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」の該当個所を参照し，記載されている［対応］に従って対応してください。
5	IPV6CP 状態が up である	相手装置との間で IPV6CP が確立しています。	「8.8　IPv6 ネットワークの通信障害」を参照してください。
6	IPV6CP 状態が down である	相手装置との間で IPV6CP が確立していません。	IPv6 アドレスコンフィグレーションが設定されているか確認してください。上記以外の場合は show logging コマンドにより表示される該当 Line のログより，「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」の該当個所を参照し，記載されている［対応］に従って対応してください。
7	OSINLCP 状態が up である	相手装置との間で対象の OSINLCP が確立しています。	「8.5　IPv4 ネットワークの通信障害」，または「8.8　IPv6 ネットワークの通信障害」を参照してください。
8	OSINLCP 状態が down である	相手装置との間で対象の NCP が確立していません。	以下の条件に該当していないか確認してください。 • isis コンフィグレーションが設定されていない。 • IP アドレスコンフィグレーションが設定されていない。 上記以外の場合は show logging コマンドにより表示される該当 Line のログより，「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」の該当個所を参照し，記載されている［対応］に従って対応してください。
9	MPLSCP 状態が up である	相手装置との間で対象の MPLSCP が確立しています。	「8.11　MPLS の通信障害【OP-MPLS】」を参照してください。

項番	PPP 状態	原因	対応
10	MPLSCP 状態が down である	相手装置との間で対象の NCP が確立していません。	mpls コンフィグレーションが設定されているか確認してください。上記以外の場合は，show logging コマンドにより表示される該当 Line のログより「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」の該当個所を参照し，記載されている［対応］に従ってください。

8.4.8　POS でのトラブル発生時の対応

POS でトラブルが発生した場合は，以下の順序で障害の切り分けを行ってください。

1. ログの確認
   ログは「メッセージ・ログレファレンス　3.5.2 イベント発生部位＝ LINEWAN」および「メッセージ・ログレファレンス　3.9 ネットワークインタフェースモジュール・イーサネット」を参照してください。
2. 障害解析方法に従った原因の切り分け
   以下の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 8-17　POS でのトラブル発生時の障害解析方法

項番	確認内容	原因	対応
1	show interfaces コマンドの障害統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • LOS • LOF • B2SD • P-LOP • B2EBER • S-BIP8 • L-BIP384 • L-BIP1536 • P-BIP8	回線クロックの同期がとれていません。	コンフィグレーションコマンド line の clock と相手装置の同期クロックの設定が正しい組み合わせか確認してください。本装置のクロックを external に指定している場合，相手装置のクロックを independent に指定してください。本装置のクロックを external に設定し，相手装置を SONET/SDH 装置とする場合，相手装置の入力周波数精度を確認してください。入力周波数精度は「解説書 Vol.1　5. POS（PPP Over SONET/SDH）」のクロックを参照してください。
		受信側の回線品質が低下しています。	光ファイバの種別が正しいか確認してください。種別は「解説書 Vol.1　5. POS（PPP Over SONET/SDH）」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「解説書 Vol.1　5. POS（PPP Over SONET/SDH）」を参照してください。
			ケーブル長を確認してください。ケーブル長は「解説書 Vol.1　5. POS（PPP Over SONET/SDH）」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合，汚れをふき取ってください。
			トランシーバを交換可能な NIF の場合，トランシーバの接続が正しいか確認してください。
			トランシーバを交換可能な NIF の場合，相手装置のトランシーバの伝送距離と合わせてください。

項番	確認内容	原因	対応
			光レベルが正しいか確認してください。光レベルは「解説書 Vol.1　5. POS（PPP Over SONET/SDH）」を参照してください。
			相手装置の送信側機能に問題ないか確認してください。相手装置に回線テスト機能がある場合，相手装置の回線テストを実行してください。
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。「運用コマンドレファレンス Vol.1　no test interfaces（POS)」の実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「9.7　回線をテストする」を参照してください。
2	show interfaces コマンドの障害統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • L-RDI • P-RDI • RDI P-AIS/P-LOP • L-REI • P-REI	回線クロックの同期がとれていません。	コンフィグレーションコマンド line の clock と相手装置の同期クロックの指定が正しい組み合わせか確認してください。本装置のクロックを external に指定している場合，相手装置のクロックを independent に指定してください。本装置のクロックを external に指定し，相手装置を SONET/SDH 装置とする場合，相手装置の入力周波数精度を確認してください。入力周波数精度は「解説書 Vol.1　5. POS（PPP Over SONET/SDH)」のクロックを参照してください。
		送信側の回線品質が低下しています。	光ファイバの種別が正しいか確認してください。種別は「解説書 Vol.1　5. POS（PPP Over SONET/SDH)」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「解説書 Vol.1　5. POS（PPP Over SONET/SDH)」を参照してください。
			ケーブル長を確認してください。ケーブル長は「解説書 Vol.1　5. POS（PPP Over SONET/SDH)」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合，汚れをふき取ってください。
			トランシーバを交換可能な NIF の場合，トランシーバの接続が正しいか確認してください。
			トランシーバを交換可能な NIF の場合，相手装置のトランシーバの伝送距離と合わせてください。
			光レベルが正しいか確認してください。光レベルは「解説書 Vol.1　5. POS（PPP Over SONET/SDH)」を参照してください。
			相手装置の受信側機能に問題ないか確認してください。相手装置に回線テスト機能がある場合，相手装置の回線テストを実行してください。
			本装置の回線テストを実行して送信側機能に問題ないか確認してください。「運用コマンドレファレンス Vol.1　no test interfaces（POS)」の実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「9.7　回線をテストする」を参照してください。

項番	確認内容	原因	対応
3	show interfaces コマンドの障害統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • RDI-PLM	RDI モードの設定が相手装置と不一致です。	コンフィグレーションコマンド line の rdi と相手装置の RDI モードの設定が一致しているか確認してください。不一致の場合，一致するように設定してください。
		スクランブルの設定，および C2 の設定が相手装置と不一致です。	コンフィグレーションコマンド line の scramble と相手装置のスクランブルの設定が一致しているか確認してください。不一致の場合，一致するように設定してください。
			スクランブルが有効または無効時の C2 が相手装置と一致しているか確認してください。C2 の設定値は「解説書 Vol.1　5.2.1　OC-192c/STM-64 POS」のフレームフォーマットの詳細情報を参照してください。
		送信側の回線品質が低下しています。	光ファイバの種別が正しいか確認してください。種別は「解説書 Vol.1　5. POS（PPP Over SONET/SDH）」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「解説書 Vol.1　5. POS（PPP Over SONET/SDH）」を参照してください。
			ケーブル長を確認してください。ケーブル長は「解説書 Vol.1　5. POS（PPP Over SONET/SDH）」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合，汚れをふき取ってください。
			トランシーバを交換可能な NIF の場合，トランシーバの接続が正しいか確認してください。
			トランシーバを交換可能な NIF の場合，相手装置のトランシーバの伝送距離と合わせてください。
			光レベルが正しいか確認してください。光レベルは「解説書 Vol.1　5. POS（PPP Over SONET/SDH）」を参照してください。
			相手装置の受信側機能に問題ないか確認してください。相手装置に回線テスト機能がある場合，相手装置の回線テストを実行してください。
			本装置の回線テストを実行して送信側機能に問題ないか確認してください。「運用コマンドレファレンス Vol.1　no test interfaces（POS)」の実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「9.7　回線をテストする」を参照してください。
4	show interfaces コマンドの障害統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • RDI P-UNEQ • P-UNEQ • P-PLM	スクランブルの設定および，C2 の設定が相手装置と不一致です。	コンフィグレーションコマンド line の scramble と相手装置のスクランブルの設定が一致しているか確認してください。不一致の場合，一致するように設定してください。

項番	確認内容	原因	対応
			スクランブルが有効または無効時の C2 が相手装置と一致しているか確認してください。C2 の設定値は「解説書 Vol.1　5.2.1 OC-192c/STM-64 POS」のフレームフォーマットの詳細情報を参照してください。
5	show interfaces コマンドの Line detail 情報により該当回線で以下の値が一致しているか確認してください。不一致の場合，原因と対応欄を参照してください。section trace message send と section trace message receive	セクショントレースメッセージが相手装置と不一致です。※	コンフィグレーションコマンド line の section_trace_message_mode と相手装置のセクショントレースメッセージの設定が一致しているか確認してください。不一致の場合，一致するように設定してください。
			コンフィグレーションコマンド line の j0 と相手装置の J0 の設定が一致しているか確認してください。不一致の場合，一致するように設定してください。
6	本装置の SS ビットと相手装置の SS ビットの設定が一致しているか確認してください。不一致の場合，原因と対応欄を参照してください。	SONET オーバヘッド内の SS ビットが相手装置と不一致です。※	コンフィグレーションコマンド line の mode と相手装置の SS ビットの設定が一致しているか確認してください。不一致の場合，一致するように設定してください。SS ビットの設定値は「解説書 Vol.1　5.2.1 OC-192c/STM-64 POS」の動作モードを参照してください。

注※　本装置は不一致の場合でも回線障害とせずに正常に動作します。相手装置が不一致の場合に回線障害とする装置であると接続できません。

8.4.9 PPP 使用時の通信障害

(1) 運用ログによる確認

PPP を使用した回線で接続ができない場合，該当回線の PPP の運用ログが show logging コマンドで表示されていないか確認してください。表示されている場合は「メッセージ・ログレファレンス　3.3.1 イベント発生部位＝ PPP」に記載している該当メッセージの [対応] を参照してください。リンク品質低下または，ネゴシエーションループのログ表示されていた場合は「(3) リンク品質低下，またはネゴシエーションループのリンク障害が発生した場合の障害解析方法」を参照してください。

(2) 統計情報による確認

次の表で示す障害解析方法から原因の切り分けを行うことができます。

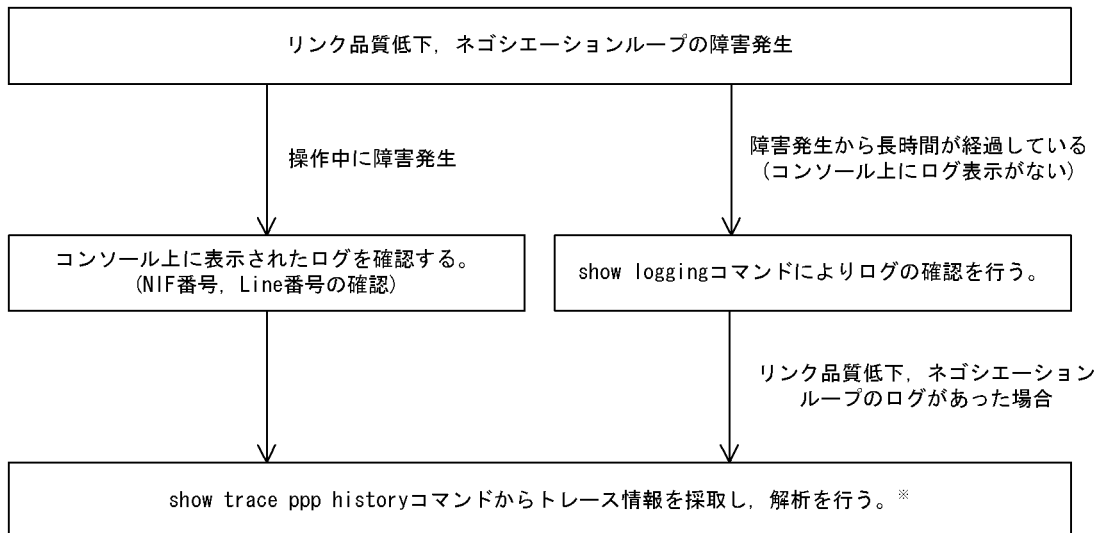
表 8-18　PPP 使用時の通信障害解析方法

項番	確認内容	原因	対応
1	show interfaces コマンドの障害統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • CRC Errors	相手装置と回線の CRC 長が一致していない可能性があります。	コンフィグレーションコマンド line の CRC 長と相手装置の CRC 長の設定が一致しているか確認してください。不一致の場合，一致するように設定してください。

項番	確認内容	原因	対応
2	show interfaces コマンドの PPP 障害統計情報により該当回線で以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • In invalid PPP pkts	本装置の LCP または，NCP 状態が down 時に相手装置から LCP，または NCP パケットを受信しています。	show trace ppp コマンドで 採取した PPP パケットのトレース情報を確認できます。表示項目のパケット採取条件種別に”Status unmatch”が表示されている場合，相手装置の PPP の設定と状態を確認してください。
		相手装置から受信した Echo-Reply パケットから無効なマジックナンバーを検出したか，Echo-Request パケットまたは Configure-Request パケットがループしている可能性があります。	本原因の場合，本装置はリンク品質監視により品質低下を検出することがあります。相手装置の PPP の実装を確認するか，パケットがループするようなネットワーク構成になっていないか確認してください。

(3) リンク品質低下，またはネゴシエーションループのリンク障害が発生した場合の障害解析方法

リンク品質低下，またはネゴシエーションループによるリンク障害が発生した場合，show trace ppp history コマンドにより障害発生直後の PPP 制御パケットのトレース情報を採取できます。次の図に障害発生から情報採取までのフローを示します。show trace ppp history コマンドの詳細は，「運用コマンドレファレンス Vol.1　show trace ppp history」を参照してください。

図 8-6　リンク品質低下，ネゴシエーションループ発生時の情報採取フロー

注※　show trace ppp history コマンドは該当回線で採取したトレース情報だけを表示するか，または装置内で保持しているトレース情報すべてを表示することが可能です。

8.5　IPv4 ネットワークの通信障害

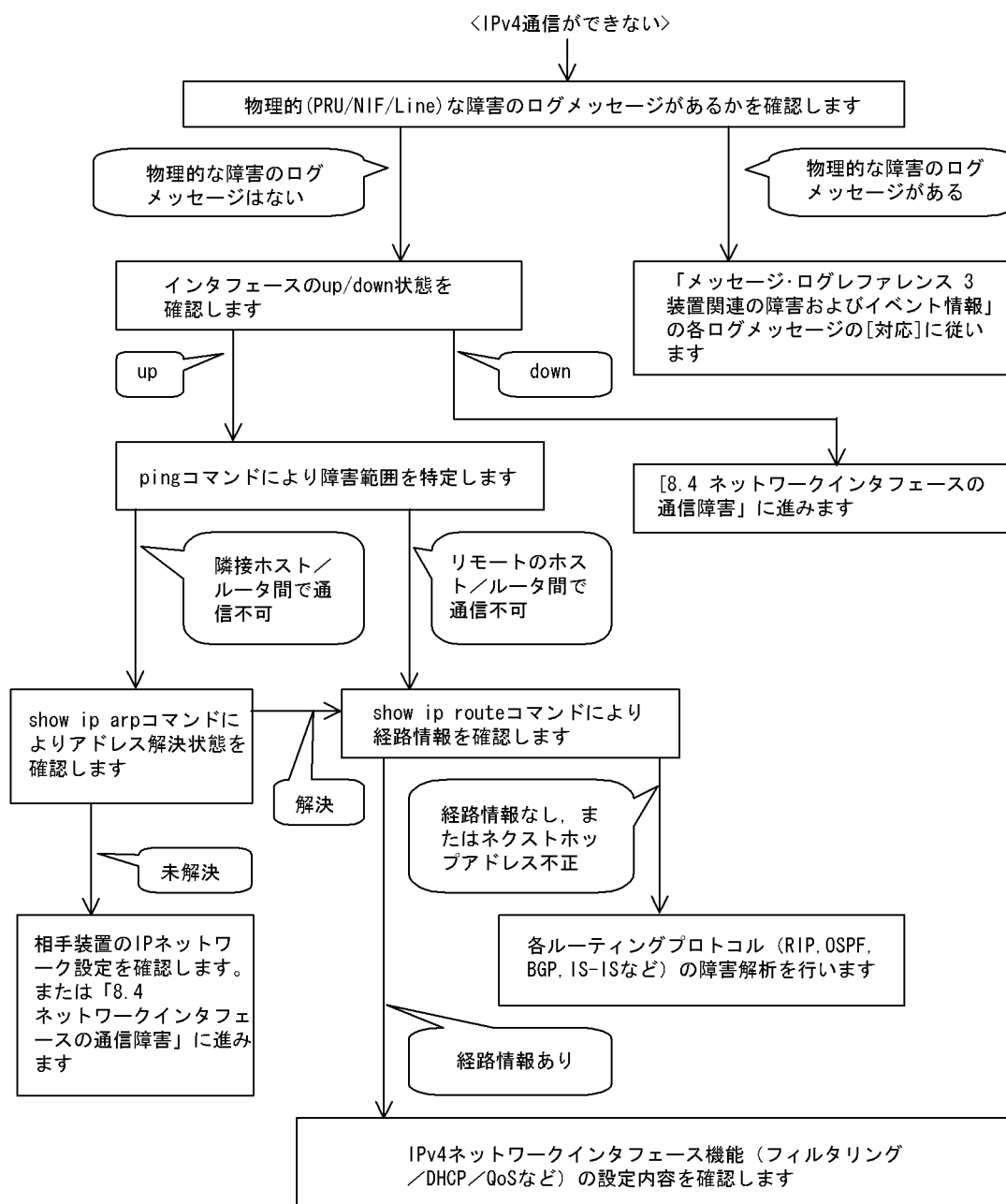
8.5.1　通信ができない，または切断されている

本装置を使用している IPv4 ネットワーク上で，通信トラブルが発生する要因として考えられるのは，次の 3 種類があります。

1. IP 通信に関係するコンフィグレーションの変更
2. ネットワークの構成変更
3. ネットワークを構成する機器の障害

上記 1. および 2. については，コンフィグレーションおよびネットワーク構成の変更前と変更後の差分を調べていただき，通信ができなくなるような原因がないか確認してください。

ここでは，3. に示すように「コンフィグレーションおよびネットワーク構成は正しいのに IP 通信ができない」，「これまで正常に動いていたのに IP 通信ができなくなった」というケースを中心に，障害部位および原因の切り分け手順を説明いたします。

障害部位および原因の切り分け方法は，次のフローに従ってください。

(1) ログの確認

通信ができなくなる原因の一つには，ハードウェア（PRU ／ NIF ／ Line）の障害（または壊れ）が考えられます。本装置が表示するログで，ハードウェアの障害を示すメッセージの表示手順を示します。

なお，ログの内容については，「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」を参照してください。

1. 本装置にログインします。
2. show logging コマンドを使ってログを表示させます。
3. ログには各々発生した日時が表示されます。通信ができなくなった日時にログが表示されていないか確認してください。
4. 通信ができなくなった日時に表示されているログの障害の内容および障害への対応は「メッセージ・ロ

グレファレンス」に記載しています。その指示に従ってください。
5. 通信ができなくなった日時にログの表示がないときは，「(2)　インタフェース状態の確認」に進んでください。

(2)　インタフェース状態の確認

本装置のハードウェアは正常に動作している場合でも，本装置と接続している隣接の装置のハードウェアに障害が発生していることも考えられます。

本装置と隣接の装置間の，インタフェースの状態を確認する手順を次に示します。

1. 本装置にログインします。
2. show ip interface コマンドを使って該当装置間のインタフェースの Up ／ Down 状態を確認してください。
3. 該当インタフェースが”Down”状態のときは，「8.4　ネットワークインタフェースの通信障害」を参照してください。
4. 該当インタフェースとの間のインタフェースが”Up”状態のときは，「(3)　障害範囲の特定（本装置から実施する場合)」に進んでください。

(3)　障害範囲の特定（本装置から実施する場合）

本装置に障害がない場合は，通信を行っていた相手との間のどこかに障害が発生している可能性があります。通信相手とのどこの部分で障害が発生しているか，障害範囲を特定する手順を次に示します。

1. 本装置にログインします。
2. ping コマンドを使って通信できない両方の相手との疎通を確認してください。ping コマンドの操作例および実行結果の見方は，「6.3.1　当該宛先アドレスとの通信可否を確認する」を参照してください。
3. ping コマンドで通信相手との疎通が確認できなかったときは，さらに ping コマンドを使って本装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping コマンド実行の結果，障害範囲が隣接装置の場合は「(5)　隣接装置との ARP 解決情報の確認」に，リモート先の装置の場合は「(6)　ユニキャストルーティング情報の確認」に進んでください。

(4)　障害範囲の特定（お客様の端末装置から実施する場合）

本装置にログインできない環境にある場合に，お客様の端末装置から通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. お客様の端末装置に ping 機能があることを確認してください。
2. ping 機能をお使いになり，お客様の端末装置と通信相手との疎通ができるか確認してください。
3. ping 機能で通信相手との疎通が確認できなかったときは，さらに ping コマンドを使ってお客様の端末装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping 機能による障害範囲が特定できましたら，障害と考えられる装置が本装置である場合は本装置にログインしていただき，障害解析フローに従って障害原因の調査を行ってください。

(5)　隣接装置との ARP 解決情報の確認

ping コマンドの実行結果によって隣接装置との疎通が不可の場合は，ARP によるアドレスが解決していないことが考えられます。本装置と隣接装置間のアドレス解決状態を確認する手順を次に示します。

1. 本装置にログインします。
2. show ip arp コマンドを使って隣接装置間とのアドレス解決状態（ARP エントリ情報の有無）を確認してください。
3. 隣接装置間とのアドレスが解決している（ARP エントリ情報あり）場合は，「(6)　ユニキャストルーティング情報の確認」に進んでください。

4. 隣接装置間とのアドレスが解決していない（ARP エントリ情報なし）場合は，隣接装置と本装置の IP ネットワーク設定が一致しているかを確認してください。

(6) ユニキャストルーティング情報の確認

隣接装置とのアドレスが解決しているにもかかわらず通信ができない場合や，IPv4 ユニキャスト通信で通信相手との途中の経路で疎通が不可となる，または通信相手までの経路がおかしいなどの場合は，本装置が取得した経路情報を確認する必要があります。確認手順を次に示します。

1. 本装置にログインします。
2. show ip route コマンドを実行して，本装置が取得した経路情報を確認してください。
3. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がない場合やネクストホップアドレスが不正の場合は「8.6　IPv4 ユニキャストルーティングの通信障害」に進んでください。
4. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がある場合は，通信不可のインタフェースに設定している次の機能に問題があると考えられます。該当する機能の調査を行ってください。
   - フィルタリング／ QoS 機能
     「(7) フィルタリング／ QoS 設定情報の確認」に進んでください。
   - ポリシールーティング機能
     「(9) ポリシールーティング設定情報の確認」に進んでください。

(7) フィルタリング／ QoS 設定情報の確認

本装置において，インタフェースが up 状態で，かつ経路情報も正しく設定されているにもかかわらず通信ができない場合は，フィルタリング機能により特定のパケットが廃棄されているか，あるいは QoS 機能の帯域制御，出力優先制御，または廃棄制御によりパケットが廃棄されている可能性があります。

したがって，スタートアップコンフィグレーションファイルのフィルタリング機能および QoS 機能の設定条件が正しいか，システム構築において帯域制御ならびに優先・廃棄制御がシステム運用において適切であるか見直してください。また，フィルタリング機能および QoS 機能によって本装置内でパケットが廃棄されている場合の，廃棄個所の特定方法の手順を次に示します。

(a) フィルタリング機能によるパケット廃棄の確認方法

1. 本装置にログインします。
2. show filter-flow コマンドを使って入出力インタフェースでパケットが廃棄されていないか確認してください。

［確認例］

通信できないパケットの入力インタフェース名称が tokyo1，送信元 IP アドレスが 170.10.11.10 の場合，フィルタリング機能で廃棄されているかどうかを確認します。

1. 本装置にログインします。
2. 「show filter-flow interface tokyo1 detail」と入力します。

```
> show filter-flow interface tokyo1 detail
<Filter IP List No.>:    1
      Using Interface:tokyo1/in
      ip source: 170.10.11.21 - 170.10.11.30
      ip destination: any
      protocol:6(tcp)
      port source:80
      ack check off
      syn check off
      forward packets                                  :                 461
```

```
<Filter IP List No.>:    2
      Using Interface:tokyo1/in
      ip source: any
      ip destination: any
      protocol:ip
      drop packets                                     :                50121
>
```

3. 入力インタフェース名称が tokyo1 の <Filter IP List No> を確認します。
   上記例では，<Filter IP List No.>:1,2 が該当します。
4. 3. で確認したフロー条件と通信できないパケットの内容を比較して，一致する <Filter IP List No.> の動作が廃棄になっていないか確認します。
   本例ではパケットの送信元 IP アドレスが 170.10.11.10 なので <Filter IP List No.>:2 と一致します。
   <Filter IP List No.>:2 の動作は廃棄なので，入力インタフェースのフィルタリング機能で廃棄されている可能性があります。

(b) QoS 機能の帯域制御によるパケット廃棄の確認方法

1. 本装置にログインします。
2. show qos ip-flow コマンドを使って入出力インタフェースでパケットが QoS 機能の帯域制御によって廃棄されていないか確認してください。

［確認例］

通信できないパケットの入力インタフェース名称が tokyo1，送信元 IP アドレスが 170.10.11.21 の場合，QoS 機能の帯域制御によって廃棄されているかどうかを確認します。

1. 本装置にログインします。
2. 「show qos ip-flow interface tokyo1 detail」と入力します。

```
>show qos ip-flow interface tokyo1 detail
<QoS IP List No.>:    1   max rate normal
      Using Interface:tokyo1/in
      ip source: 170.10.11.21 - 170.10.11.30
      ip destination: any
      protocol:ip
      burst size:3000Byte
      packets of     100000kbps and under(priority3 discard4)
                                                       :                 7021
      packets of     100000kbps over     (drop)
                                                       :                  729
<QoS IP List No.>:    2
      Using Interface: tokyo1/out
      ip source: any
      ip destination: any
      protocol:6(tcp)
      port destination:20 - 21
      ack check off
      syn check off
      hit packets                    (priority8 discard4)
                                                       :             11568793
>
```

3. 入力インタフェース名称が tokyo1 の <QoS IP List No.> を確認します。
   上記例では <QoS IP List No.>:1 が該当します。
4. 3. で確認したフロー条件と通信できないパケットの内容を比較して，一致する <QoS IP List No.> の動作が廃棄になっていないか確認します。
   本例ではパケットの送信元 IP アドレスが 170.10.11.21 なので，<QoS IP List No.>:1 と一致します。
   <QoS IP List No.>:1 の契約帯域違反時 (packets of 1000000bps over (drop)) の動作は廃棄なので，入力インタフェースの QoS 機能の帯域制御で廃棄されている可能性があります。

(c) QoS 機能のキュー制御によるパケット廃棄の確認方法

1. 本装置にログインします。
2. show qos queueing コマンドを使って出力インタフェースでパケットが QoS 機能のキュー制御によって廃棄されていないか確認してください。

［確認例］

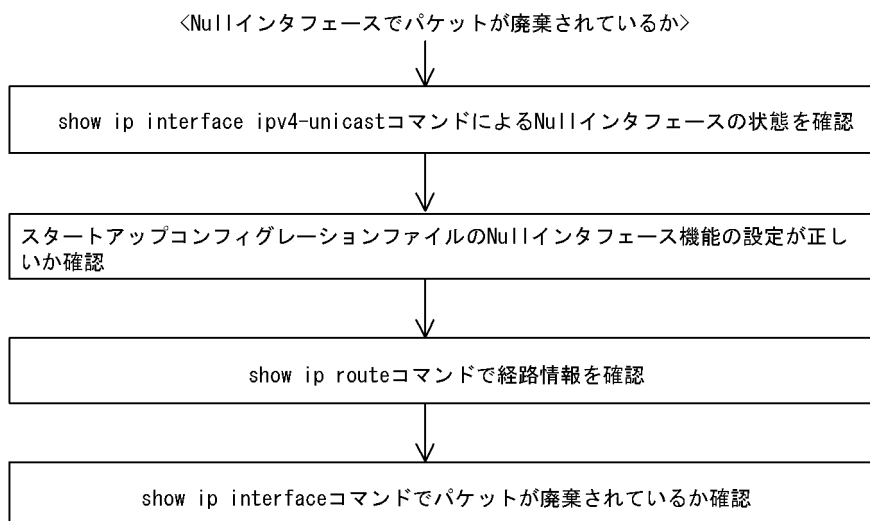
QoS 機能のキュー制御によって廃棄されているかどうかを確認します。通信できないパケットの出力インタフェースが NIF 番号 0，Line 番号 1，使用するキュー番号が 4（Priority 4）の場合での確認方法を以下に示します。

1. 本装置にログインします。
2. 「show qos queueing nif 0 line 1」と入力します。

```
> show qos queueing nif 0 line 1
NIF0/Line1 (outbound), Rate_limit=1000kbps, Qmode=Priority
 Max_Queue=8
                              :
                              :
  Priority(Queue)=4, Qlen=1, Maximum_Qlen=2, Limit_Qlen=127
   Discard       send_pkt    discard_pkt      send_byte   discard_byte
   1                 6533             19         533.0k          10.0k
   2                 2564           1581         125.5M          20.0k
   3              2256877           1235        5433.2M          10.0k
   4               568788           2548         255.0k          20.0k
   total          2834762           5383        5559.6M          60.0k
                              :
                              :
>
```

3. Priority 4 での廃棄したパケット数（discard_pkt）の total 値が 1 以上の場合，キュー制御によってパケットが廃棄されています。本例では 5383 なので，キュー制御によってパケットが廃棄されています。

(8) Null インタフェース設定情報の確認

特定のネットワーク宛または特定の端末宛の通信を Null インタフェースに向けて制限しているにもかかわらず，パケットが廃棄されない場合は，Null インタフェースの設定内容に誤りがある可能性があります。次の手順で Null インタフェースの設定内容が正しいか確認してください。

1. show ip interface ipv4-unicast コマンドを使い Null インタフェースの状態を確認します。Null インタフェースが UP しているか確認してください。
2. スタートアップコンフィグレーションファイルで Null インタフェースが定義されているか確認します。
3. show ip route コマンドで経路情報を確認します。
   コンフィグレーションコマンド static で定義した経路情報の設定内容が正しいかどうかを確認してください。
4. パケットが廃棄されているか確認します。
   show ip interface コマンドを使って Null インタフェースでパケットが廃棄されているか確認してください。

(9) ポリシールーティング設定情報の確認

本装置において物理的障害は発生してなく，経路情報も正しく設定されているにもかかわらず通信ができない場合は，ポリシールーティング機能の出力先インタフェースに障害が発生しているためにパケットが廃棄されている可能性が考えられます。

したがって，次の手順でポリシールーティングの現在使用されている出力先インタフェースの状態を確認してください。

(a) ポリシールーティング機能による出力先インタフェースの確認方法

1. 本装置にログインします。
2. show ip policy コマンドを使って入力インタフェースのポリシールーティング設定内容と，現在使用されている出力先インタフェースの状態を確認します。

［確認例］

通信できないパケットの入力インタフェースが tokyo，送信元 IP アドレスが 200.1.4.5 の場合，ポリシールーティング機能で使用されている出力先を確認します。

1. 本装置にログインします。
2. 「show ip policy interface tokyo」と入力します。

```
> show ip policy interface tokyo
<Interface Name>            <Filter List No>
  tokyo                      1,2
>
```

3. 入力インタフェース tokyo で使用されている条件番号を確認します。
   上記例では，＜ Filter List No. ＞ :1,2 が該当します。
4. 3. で確認した条件の詳細を表示します。「show ip local policy interface tokyo 1 2」と入力します。

```
> show ip local policy interface tokyo 1 2
<Interface Name>: tokyo           <Filter List No.> 1
        forward packets
        protocol                  : ip
        ip_source                 : 200.1.4.0 - 200.1.4.255
        ip_destination            : 200.1.7.0 - 200.1.8.255
        current policy route
          Policy Group Name         route1
          Output Interface          tokyo3
          Next Hop IP address       200.1.10.1
<Interface Name>: tokyo           <Filter List No.> 2
        forward packets
        protocol                  : ip
        ip_source                 : 200.1.5.0 - 200.1.5.255
        ip_destination            : 200.1.19.0 - 200.1.20.255
        current policy route
          Policy Group Name         route2
          Output Interface          yokohama
          Next Hop IP address       200.1.50.2
```

```
>
```

5. 各条件の内容と条件とその際の出力先を確認します。
   通信できないパケットの内容を比較して，一致する条件のポリシールーティンググループ名称を確認します。
6. 採用されているポリシーグループの状態を確認します。「show ip cache policy route1」と入力します。

```
> show ip cache policy route1
<Policy Group Name>:     route1
       priority  Interface Name  status   Nexthop
           1     tokyo1            Down   200. 1. 1.  2
           2     tokyo1            Down   200. 1. 2.  2
           3     tokyo2            Down   200. 1. 8.  3
   *>      4     tokyo3            Down   200. 1. 10. 1    default
>
```

7. 出力先インタフェースが障害により出力できないためパケットが廃棄されています。スタートアップコンフィグレーションファイルのポリシー情報の設定を見直すと共に，「8.4　ネットワークインタフェースの通信障害」に従ってください。
   なお，show ip cache policy コマンド実行時，使用中の経路がない（経路の先頭に *> の表示がない）場合も，出力先インタフェースの障害によりパケットが廃棄されていることを表します。

（10）Tag-VLAN 連携設定情報の確認

本装置に，IP インタフェース情報，経路情報が正しく設定されているにもかかわらず通信ができない場合は，Tag-VLAN 連携情報の設定が誤っている（またはされていない）ために，パケットが廃棄されている可能性が考えられます。本装置の Tag-VLAN 連携設定情報を確認する手順を次に示します。

1. 本装置にログインします。
2. show interfaces コマンドを使用して Tag-VLAN 連携設定情報（Tag-VLAN 連携機能の使用の有無，Tag-VLAN 連携回線情報および VLAN ID）を確認してください。

上記コマンドで Tag-VLAN 連携の設定が正しいと確認できた場合は，本装置に関する Tag-VLAN 連携の設定に問題はありません。接続装置（LAN Switch など）の設定に問題（VLAN 設定をしていない，VLAN ID が一致していない）がある可能性があります。接続装置の設定情報を確認してください。

8.5.2　DHCP 機能で IP アドレスが割り振られない

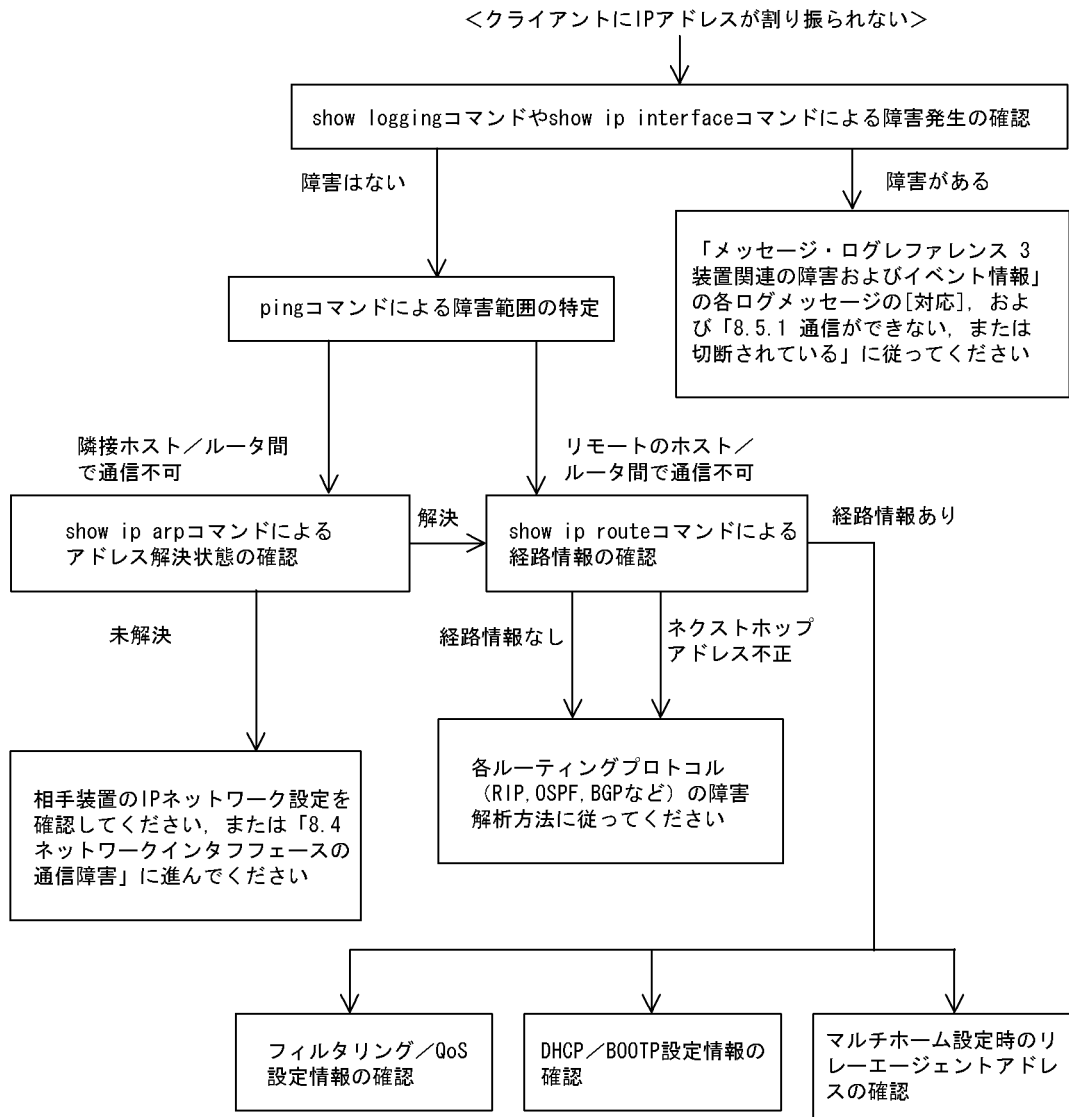
（1） DHCP ／ BOOTP リレーの通信トラブル

DHCP ／ BOOTP リレーの通信トラブルが発生する要因として考えられるのは，次の 3 種類があります。

1. DHCP ／ BOOTP リレー通信に関係するコンフィグレーションの変更
2. ネットワークの構成変更
3. DHCP ／ BOOTP サーバの障害

上記 2. については，ネットワーク構成の変更前と変更後の差分を調べていただき，通信ができなくなるような原因がないか確認してください。

ここでは，クライアントの設定（ネットワークカードの設定，ケーブルの接続など）は確認されているものとし，上記 1. および 3. に示すような「コンフィグレーションの変更を行ったら，DHCP ／ BOOTP サーバから IP アドレスが割り振られなくなった」，「コンフィグレーションおよびネットワーク構成は正しいのにクライアントに IP アドレスが割り振られず，IP 通信できない」，というケースについて，障害部位および原因の切り分け手順を説明いたします。

障害部位および原因の切り分け方法は，次のフローに従ってください。

(a)　ログおよびインタフェースの確認

クライアントに IP アドレスが割り振られなくなる原因の一つにクライアント - サーバ間で通信ができなくなっていることが考えられます。本装置が表示するログや show ip interface コマンドによるインタフェースの up ／ down 状態を確認してください。手順については「8.5.1　通信ができない，または切断されている」を参照してください。

(b)　障害範囲の特定（本装置から実施する場合）

本装置に障害がないときは通信を行っていた相手との間のどこかに障害が発生している可能性があります。通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. 本装置にログインします。
2. ping コマンドを使って通信できない両方の相手との疎通を確認してください。ping コマンドの操作例および実行結果の見方は，「6.3.1　当該宛先アドレスとの通信可否を確認する」を参照してください。
3. ping コマンドで通信相手との疎通が確認できなかったときは，さらに ping コマンドを使って本装置に近い装置から順に通信相手に向けて疎通を確認してください。

4. ping コマンド実行の結果，障害範囲が隣接装置の場合は「(d) 隣接装置との ARP 解決情報の確認」に，リモート先の装置の場合は「(e) 経路情報の確認」に進んでください。

(c) 障害範囲の特定（お客様の端末装置から実施する場合）

本装置にログインできない環境にある場合に，お客様の端末装置から通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. お客様の端末装置に ping 機能があることを確認してください。
2. ping 機能をお使いになり，お客様の端末装置と通信相手との疎通ができるか確認してください。
3. ping 機能で通信相手との疎通が確認できなかったときは，さらに ping コマンドを使ってお客様の端末装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping 機能による障害範囲の特定ができましたら，障害と考えられる装置が本装置である場合は本装置にログインしていただき，障害解析フローに従って障害原因の調査を行ってください。

(d) 隣接装置との ARP 解決情報の確認

ping コマンドによって隣接装置との疎通が不可のときは，ARP によるアドレスが解決していないことが考えられます。本装置と隣接装置間のアドレス解決状態を確認する手順を次に示します。

1. 本装置にログインします。
2. show ip arp コマンドを使って隣接装置間とのアドレス解決状態（ARP エントリ情報の有無）を確認してください。
3. 隣接装置間とのアドレスが解決している（ARP エントリ情報あり）場合は，「(e) 経路情報の確認」に進んでください。
4. 隣接装置間とのアドレスが解決していない（ARP エントリ情報なし）場合は，隣接装置と本装置の IP ネットワーク設定が疎通できる設定になっているかを確認してください。

(e) 経路情報の確認

隣接装置とのアドレスが解決しているにもかかわらず通信ができない，通信相手との途中の経路で疎通が不可となる，または通信相手までの経路がおかしいなどの場合は，本装置が取得した経路情報を確認する必要があります。確認手順を次に示します。

1. 本装置にログインします。
2. show ip route コマンドを使って本装置が取得した経路情報を確認してください。
3. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がない場合やネクストホップアドレスが不正の場合は「8.6 IPv4 ユニキャストルーティングの通信障害」に進んでください。
4. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がある場合は，通信不可のインタフェースに設定している次の機能に問題があると考えられます。該当する機能の調査を行ってください。
   - フィルタリング／ QoS 機能
     「(f) フィルタリング／ QoS 設定情報の確認」に進んでください。
   - DHCP ／ BOOTP 機能
     「(g) DHCP ／ BOOTP 設定情報の確認」に進んでください。
   - マルチホーム機能
     「(h) マルチホーム設定時の DHCP ／ BOOTP リレーエージェント機能情報の確認」に進んでください。

(f) フィルタリング／ QoS 設定情報の確認

本装置において，物理的障害がなく，経路情報も正しく設定されているにもかかわらず通信ができない場

合は，フィルタリング機能により特定のパケットだけを廃棄する設定になっているか，QoS 機能の帯域制御，出力優先制御または廃棄制御によりパケットが廃棄されている可能性があります。

したがって，コンフィグレーションのフィルタリング機能および QoS 機能の設定条件が正しいか，システム構築において帯域制御，出力優先制御，または廃棄制御がシステム運用において適切であるかを確認してください。

(g) DHCP ／ BOOTP 設定情報の確認

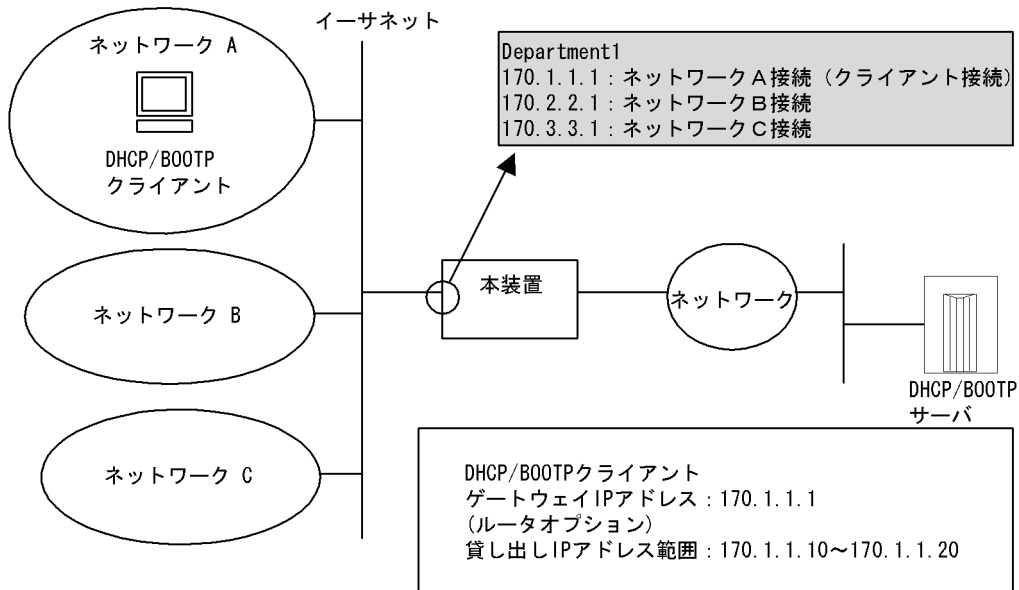
DHCP ／ BOOTP サーバに貸し出し用 IP アドレスが十分に残っている場合，DHCP ／ BOOTP リレーのコンフィグレーション設定ミスによりクライアントに IP アドレスが割り振られないという原因が考えられます。次にコンフィグレーションの確認手順を示します。

1. relay list は DHCP ／ BOOTP サーバの IP アドレス，または DHCP ／ BOOTP リレーエージェント機能付き次ルータの IP アドレスが指定されているか確認してください。
2. クライアント側のインタフェースに relay-interface が設定されているか確認してください。
3. 該当クライアントへ IP アドレスを貸与させたい DHCP ／ BOOTP サーバの IP アドレスが，relay list へ登録されており，かつそのリレーリストの登録された relay group が，リレーインタフェースに設定されているかを確認してください。
4. relay interface の bootp hops 値がクライアントから見て正しい bootp hops 値となっているか確認してください。

(h) マルチホーム設定時の DHCP ／ BOOTP リレーエージェント機能情報の確認

DHCP ／ BOOTP サーバでは，DHCP ／ BOOTP REQUEST パケット内 giaddr の IP アドレスから貸し出し IP アドレスを選択しています。

本装置において，DHCP ／ BOOTP クライアント接続インタフェースにマルチホームの設定がある場合，relay_agent_address パラメータを省略するとインタフェースに最後に IP 定義した IP アドレスを，リレーエージェントアドレスとして DHCP ／ BOOTP REQUEST パケット内 giaddr に設定しています。

DHCP ／ BOOTP クライアントが接続されているインタフェースにマルチホームが設定されている場合において，「リレーエージェントアドレス」と「DHCP ／ BOOTP クライアントが接続されている本装置設定 IP アドレス」が一致していない場合，DHCP ／ BOOTP サーバで対象貸し出し IP アドレスが識別できず，DHCP ／ BOOTP クライアントに IP アドレスの貸し出しが行われない可能性があります。この場合，show dhcp giaddr コマンドを実行し，出力された IP アドレスが，DHCP ／ BOOTP クライアントが接続されている本装置設定 IP アドレスと一致しているか確認してください。

上記構成において，show dhcp giaddr コマンドを入力したとき以下のように出力された場合，リレーエージェントアドレスと DHCP ／ BOOTP クライアントが接続されている IP アドレスとが一致していないため，IP アドレスの貸し出しが行われません。

```
> show dhcp giaddr interface Department1
DHCP GIADDR < Department1> : 170.2.2.1
>
```

一致していない場合，次の手順に従って DHCP ／ BOOTP リレーエージェント機能で適用するリレーエージェントアドレスの変更を行ってください。なお，DHCP ／ BOOTP クライアント接続インタフェースの IP コンフィグレーションを再設定するため，DHCP ／ BOOTP クライアント接続セグメントの運用を一時的に停止することになります。

［IP コンフィグレーション再設定方法］

1. インタフェースの IP 定義からクライアントが接続されている IP アドレスを削除してください（IP 定義内の IP アドレスがすべて削除されてしまう場合は relay-interface を先に削除してください）。

```
(config)# show
line Department1 ethernet 0/0
  ip 170.2.2.1/24
  ip-address 170.1.1.1/24
  ip-address 170.3.3.1/24
!
relay_list 1 170.10.10.10
relay_group BlueGroup 1
relay-interface Department1 relay_group BlueGroup
!
(config)# line Department1 ethernet 0/0
[line Department1]
(config)# delete ip-address 170.1.1.1/24
Are you sure? (y/n): y
[line Department1]
(config)# show ip
ip 170.2.2.1/24
  ip-address 170.3.3.1/24
!
(config)#
```

2. インタフェースにクライアントが接続されている IP アドレスを再設定します。

コンフィグレーションコマンド show で変更した IP 定義を表示したとき，クライアントが接続されている IP アドレスが一番下に表示されていることを確認してください。

```
[line Department1]
(config)# show ip
ip 170.2.2.1/24
  ip-address 170.3.3.1/24
!
[line Department1]
(config)# ip-address 170.1.1.1/24
[line Department1]
(config)# show ip
ip 170.2.2.1/24
ip-address 170.3.3.1/24
ip-address 170.1.1.1/24
!
[line Department1]
(config)#
```

3. コンフィグレーションモードを quit で終了し，show dhcp giaddr を実行してください。出力結果が 2. で入力した IP アドレスとなっていることを確認してください。

```
(config)# quit
# show dhcp giaddr interface Department1
DHCP GIADDR < Department1 >:  170.1.1.1
#
```

出力結果が 2. で入力した IP アドレスとなっていない場合は，次の手順に従って IP 定義と relay-interface の再設定を行ってください。なお，IP コンフィグレーションの再設定を行うため，該当インタフェースの運用を一時的に停止することになります。

(3-1)

インタフェースに設定してある relay-interface 定義を削除後，インタフェースの IP 定義をすべて削除してください。

```
(config)# delete relay-interface Department1
Are you sure? (y/n): y
(config)# line Department1 ethernet 0/0
[line Department1]
(config)# delete ip
Are you sure? (y/n): y
[line Department1]
(config)# exit
(config)# show
line Department1 ethernet 0/0
!
relay_list 1 170.10.10.10
relay_group BlueGroup 1
!
(config)#
```

(3-2)

インタフェースにクライアントが接続されている IP アドレス以外の IP アドレスを IP 登録します。

```
(config)# line Department1 ethernet 0/0
[line Department1]
(config)# ip 170.2.2.1/24
[line Department1]
(config)# ip-address 170.3.3.1/24
[line Department1]
(config)# exit
(config)# show
line Department1 ethernet 0/0
```

```
  ip 170.2.2.1/24
  ip-address 170.3.3.1/24
!
relay_list 1 170.10.10.10
relay_group BlueGroup 1
!
(config)#
```

(3-3) 最後にクライアントが接続されている IP アドレスを IP 登録してください。

```
(config)# line Department1 ethernet 0/0
[line Department1]
(config)# ip-address 170.1.1.1/24
[line Department1]
(config)# exit
(config)# show
line Department1 ethernet 0/0
  ip 170.2.2.1/24
  ip-address 170.3.3.1/24
  ip-address 170.1.1.1/24
!
relay_list 1 170.10.10.10
relay_group BlueGroup 1
!
(config)#
```

(3-4) インタフェースに relay-interface の設定を行ってください。

```
(config)# relay-interface Department1 relay_group BlueGroup
(config)# show
line Department1 ethernet 0/0
  ip 170.2.2.1/24
  ip-address 170.3.3.1/24
  ip-address 170.1.1.1/24
!
relay_list 1 170.10.10.10
relay_group BlueGroup 1
relay-interface Department1 relay_group BlueGroup
!
(config)#
```

(3-5)

show dhcp giaddr コマンドを実行し，(3-3) で入力した IP アドレスが表示されることを確認してください。

```
(config)# quit
# show dhcp giaddr interface Department1
DHCP GIADDR < Department1 >:  170.1.1.1
#
```

(i) DHCP リレーと VRRP が同一インタフェースで運用されている場合の確認

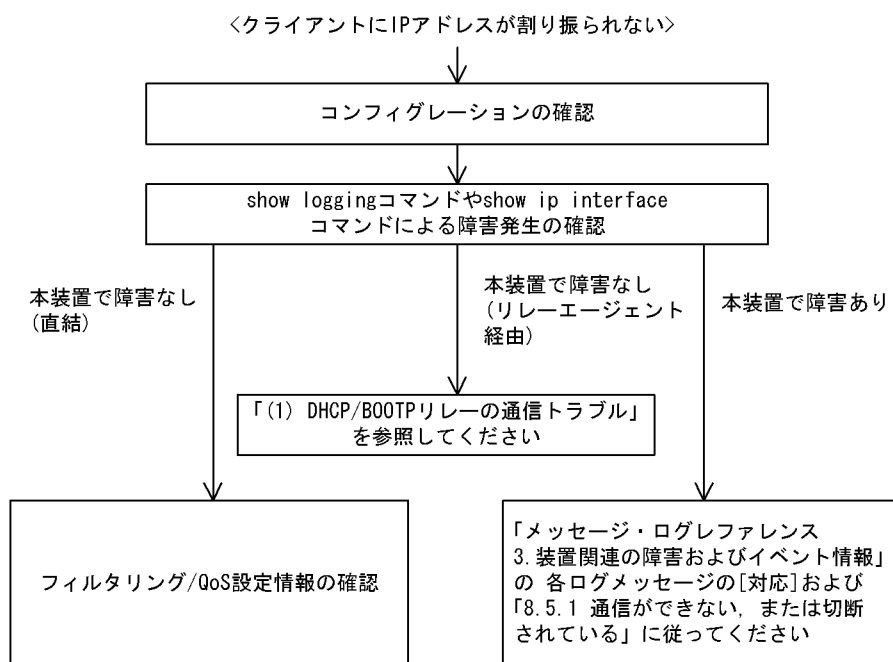
DHCP ／ BOOTP リレーと VRRP が同一インタフェースで運用されている場合，DHCP ／ BOOTP サーバにおいて，DHCP ／ BOOTP クライアントゲートウェイアドレス（ルータオプション）を VRRP コンフィグレーションで設定した仮想ルータアドレスに設定しなければなりません。設定しなかった場合，VRRP によるマスタ・スタンバイルータ切り替え後，DHCP ／ BOOTP クライアントが通信できなくなる可能性があります。確認方法については各 DHCP ／ BOOTP サーバの確認方法に従ってください。

(2) DHCP サーバの通信トラブル

DHCP サーバの通信トラブル（クライアントにアドレス配信できない）が発生する要因として考えられるのは，次の 3 種類があります。

1. コンフィグレーションの設定ミス
2. ネットワークの構成変更
3. DHCP サーバの障害

まず上記 1. の確認を行ってください。コンフィグレーションの設定で間違えやすいものを例にとり説明します。上記 2. については，ネットワーク構成の変更前と変更後の差分を調べていただき，通信ができなくなるような原因がないか確認してください。クライアント／サーバの設定（ネットワークカードの設定，ケーブルの接続など）は確認されている場合，上記 3. に示すような「コンフィグレーションおよびネットワーク構成は正しいのにクライアントに IP アドレスが割り振られず，IP 通信できない」，というケースについては，詳細を「(b) ログメッセージおよびインタフェースの確認」～「(e) フィルタリング／ QoS 設定情報の確認」に示します。

障害部位および原因の切り分け手順を次のフローに示します。

(a) コンフィグレーションの確認

DHCP サーバ上のリソース類のコンフィグレーション設定ミスによりクライアントに IP アドレスが割り振られないという原因が考えられます。コンフィグレーションの確認手順を次に示します。

1. DHCP クライアントに割り付ける IP アドレスの範囲指定（range パラメータ）が同時に使用するクライアントの台数分確保してあるかを，コンフィグレーションで確認してください。
2. 固定 IP アドレスを割り付ける PC に IP アドレス配信ができない場合，コンフィグレーションの動的に割り付ける IP アドレスの範囲指定の中にコンフィグレーションコマンド dhcp host で指定した固定 IP アドレス（fixed-address パラメータ）が含まれていないかを確認してください。アドレスが競合している可能性があります。

例えば下記の例では，動的に割り当てるアドレスを 192.168.10.100 から 192.168.10.120 で定義していますが，この範囲内に固定に割り付けるアドレス（192.168.10.110）が含まれています。192.168.10.110 のアドレスを動的に割り当てるアドレスとして先に使用した場合，アドレスを固定に割り付けたいホストには 192.168.10.110 を割り当てられません。

＜固定割り付けアドレスと動的割り付けアドレスの競合例＞

```
dhcp subnet 192.168.10.0/24 range 192.168.10.100 192.168.10.120
dhcp host manager hardware 00:11:11:ef:ff:11 fixed-address 192.168.10.110
```

1. クライアントが本装置からアドレスを割り振られたあと，クライアントと他装置との通信ができない場合は，デフォルトルータの設定がされていない場合があります。dhcp option routers でクライアントが接続されているネットワークのルータアドレス（デフォルトルータ）が設定されているか確認してください（「コンフィグレーションコマンドレファレンス Vol.1　13. DHCP サーバ情報」を参考にしてください）。
2. DHCP リレーエージェントとなる装置の設定を確認してください。リレーエージェントも本装置を使用している場合，「(1) DHCP ／ BOOTP リレーの通信トラブル」を参照してください。
3. DHCP サーバデーモンの起動がうまくできていない場合もあります。DHCP サーバに関するコンフィグレーション設定時は再起動操作が必要になります。これらの起動方法の手順は，「コンフィグレーションコマンドレファレンス Vol.1　dhcp（DHCP サーバ情報）」を参照してください。

(b) ログメッセージおよびインタフェースの確認

クライアントに IP アドレスが割り振られなくなる原因の一つにクライアント - サーバ間で通信ができなくなっていることが考えられます。本装置が表示するログメッセージや show ip interface コマンドによるインタフェースの up ／ down 状態を確認してください。手順については「8.5.1　通信ができない，または切断されている」を参照してください。

(c) 障害範囲の特定（本装置から実施する場合）

本装置に障害がないときは通信を行っていた相手との間のどこかに障害が発生している可能性があります。通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. 本装置にログインします。
2. クライアントとサーバ間にルータなどがある場合，ping コマンドを使って通信できない相手（DHCP クライアント）との間にある装置（ルータ）の疎通を確認してください。ping コマンドで通信相手との疎通が確認できなかったときは，さらに ping コマンドを使って本装置からクライアント側に向けて近い装置から順に通信相手に向けて疎通を確認してください。ping コマンドの操作例および実行結果の見方は，「6.3.1　当該宛先アドレスとの通信可否を確認する」を参照してください。
3. サーバとクライアントが直結の場合，HUB やケーブルの接続を確認してください。
4. ping コマンドによる障害範囲が隣接装置かリモートの装置かによって，障害解析フローの次のステップに進んでください。

(d) 経路情報の確認

隣接装置とのアドレスが解決しているにもかかわらず通信ができない，通信相手との途中の経路で疎通が不可となる，または通信相手までの経路がおかしいなどの場合は，本装置が取得した経路情報を確認する必要があります。確認手順を次に示します。

1. 本装置にログインします。
2. show ip route コマンドを使って本装置が取得した経路情報を確認してください。

(e) フィルタリング／ QoS 設定情報の確認

本装置において物理的障害がなく，経路情報も正しく設定されているにもかかわらず通信ができない場合は，フィルタリング機能により特定のパケットだけが廃棄されているか，あるいは QoS 機能の帯域制御，出力優先制御または廃棄制御によりパケットが廃棄されている可能性があります。したがって，コンフィグレーションのフィルタリング機能および QoS 機能の設定条件が正しいか，システム構築において帯域制御，出力優先制御または廃棄制御がシステム運用において適切であるか，本装置およびクライアント・サーバ間にある中継装置でも見直しを行ってください。

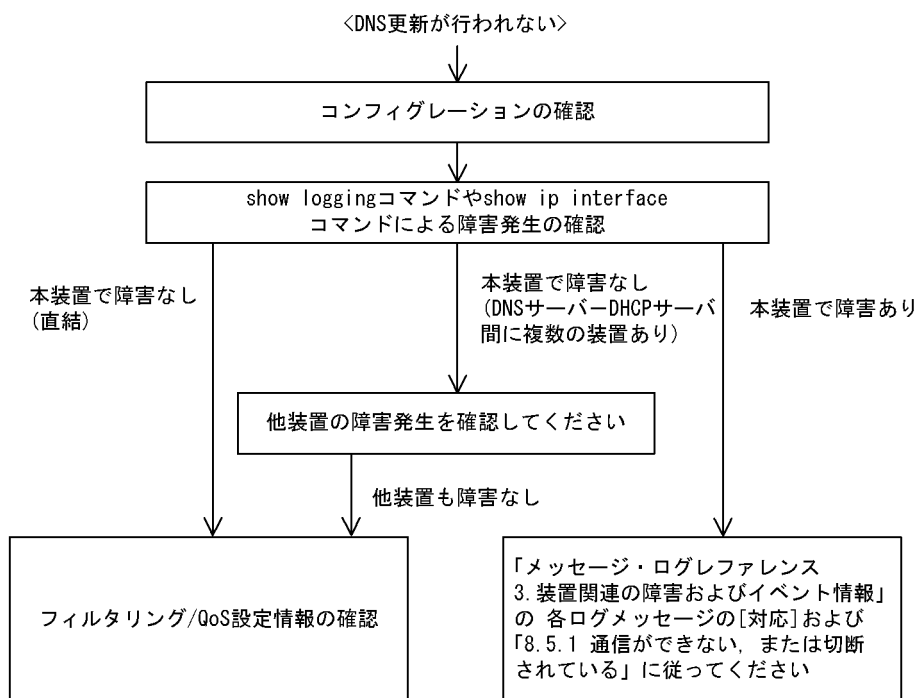
8.5.3　DHCP 機能で DynamicDNS 連携が動作しない

(1)　DHCP サーバの通信トラブル

DHCP サーバの通信トラブルが発生する要因として考えられるのは，次の 3 種類があります。

1. コンフィグレーションの設定ミス
2. ネットワークの構成変更
3. DHCP サーバの障害

まず上記 1. の確認を行ってください。コンフィグレーションの設定で間違えやすいものを例にとり説明します。上記 2. については，ネットワーク構成の変更前と変更後の差分を調べていただき，通信ができなくなるような原因がないか確認してください。DNS サーバ／ DHCP サーバの設定（ネットワークカードの設定，ケーブルの接続など）は確認されている場合，上記 3. に示すような「コンフィグレーションおよびネットワーク構成は正しいのに DynamicDNS 連携が動作しない」，というケースについては，詳細を「(b)　時刻情報の確認」～「(f)　フィルタリング／ QoS 設定情報の確認」に示します。

障害部位および原因の切り分け手順を次のフローに示します。

(a)　コンフィグレーションの確認

DHCP サーバ上のミス，または DNS サーバ上の設定との不一致によって DynamicDNS に対する DNS 更新が正しく動作していない原因が考えられます。コンフィグレーションの確認手順を次に示します。

1. 初めに DNS サーバ側で DNS 更新を許可する方法を確認してください。IP アドレス／ネットワークによるアクセス許可の場合は項目 3 以降を参照してください。認証キーによる許可の場合は項目 2 以降を参照してください。
2. DNS サーバ側で指定しているキー情報，認証キーと DHCP サーバコンフィグレーションで設定されている key 情報が同じであることを確認してください（「コンフィグレーションコマンドレファレンス Vol.1　dhcp key（DHCP DNS 認証キー情報）」を参考にしてください）。

3. DNS サーバ側で指定しているゾーン情報と DHCP サーバコンフィグレーションのゾーン情報が一致していることを確認してください（「コンフィグレーションコマンドレファレンス Vol.1　dhcp zone（DHCP DNS ゾーン情報）」を参考にしてください)。また。このときに正引きと逆引きの両方が設定されていることを確認してください。
4. DNS 更新が定義されていることを確認してください（「コンフィグレーションコマンドレファレンス Vol.1　dhcp ddns-update-enable（DHCP DNS 更新有効情報）」を参考にしてください)。デフォルトでは DNS 更新は無効になっているため，DNS 更新を行う場合は本定義を設定する必要があります。
5. クライアントが使用するドメイン名が DNS サーバに登録してあるドメイン名と一致していることを確認してください。DHCP によってドメイン名を配布する場合はコンフィグレーションで正しく設定されていることを確認してください（「コンフィグレーションコマンドレファレンス Vol.1　dhcp option（DHCP オプション情報）」および「運用コマンドレファレンス Vol.2　show ip dhcp import」を参考にしてください)。

(b) 時刻情報の確認

DNS 更新で認証キーを使用するとき，本装置と DNS サーバが指す時刻の差は多くの場合 UTC 時間で 5 分以内である必要があります。show calendar コマンドで本装置の時刻情報を確認して，必要ならば「コンフィグレーションコマンドレファレンス Vol.2　11. NTP 情報」を参考に時刻情報の同期を行ってください。

(c) ログメッセージおよびインタフェースの確認

DNS サーバとの通信ができなくなる原因の一つに DNS サーバ -DHCP サーバ間で通信ができなくなっていることが考えられます。本装置が表示するログメッセージや show ip interface コマンドによるインタフェースの up ／ down 状態を確認してください。手順については「8.5.1　通信ができない，または切断されている」を参照してください。

(d) 障害範囲の特定（本装置から実施する場合）

本装置に障害がないときは通信を行っていた相手との間のどこかに障害が発生している可能性があります。通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. 本装置にログインします。
2. DNS サーバと DHCP サーバ間にルータなどがある場合，ping コマンドを使って通信できない相手（DNS サーバ）との間にある装置（ルータ）の疎通を確認してください。ping コマンドで通信相手との疎通が確認できなかったときは，さらに ping コマンドを使って本装置からクライアント側に向けて近い装置から順に通信相手に向けて疎通を確認してください。ping コマンドの操作例および実行結果の見方は，「6.3.1　当該宛先アドレスとの通信可否を確認する」を参照してください。
3. DNS サーバと DHCP サーバが直結の場合，HUB やケーブルの接続を確認してください。
4. ping コマンドによる障害範囲が隣接装置かリモートの装置かによって，障害解析フローの次のステップに進んでください。

(e) 経路情報の確認

隣接装置とのアドレスが解決しているにもかかわらず通信ができない，通信相手との途中の経路で疎通が不可となる，または通信相手までの経路がおかしいなどの場合は，本装置が取得した経路情報を確認する必要があります。確認手順を次に示します。

1. 本装置にログインします。
2. show ip route コマンドを使って本装置が取得した経路情報を確認してください。

(f) フィルタリング／ QoS 設定情報の確認

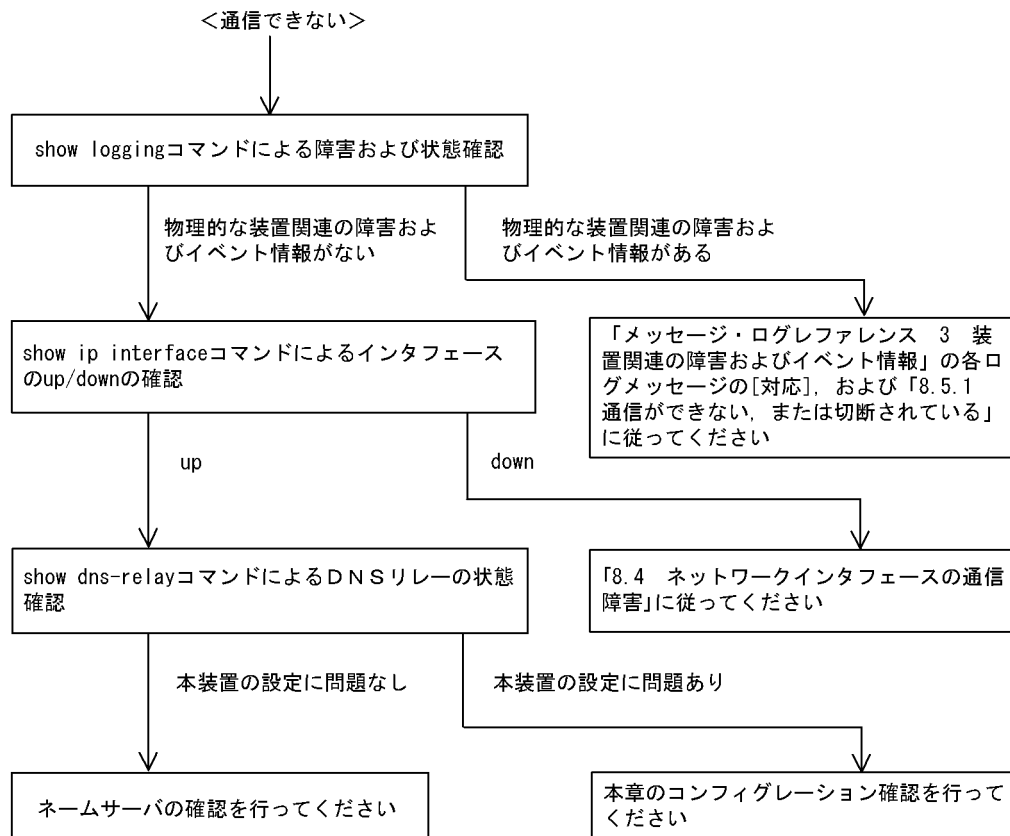
本装置において物理的障害がなく，経路情報も正しく設定されているにもかかわらず通信ができない場合

は，フィルタリング機能により特定のパケットだけが廃棄されているか，あるいは QoS 機能の帯域制御，出力優先制御または廃棄制御によりパケットが廃棄されている可能性があります。したがって，コンフィグレーションのフィルタリング機能および QoS 機能の設定条件が正しいか，システム構築において帯域制御，出力優先制御または廃棄制御がシステム運用において適切であるか，本装置および DNS サーバ・DHCP サーバ間にある中継装置でも見直しを行ってください。

8.5.4　DNS リレー通信でドメイン解決ができない

DNS リレーの通信トラブル（ドメイン解決ができない）の発生要因として考えられるのは，次の 3 種類があります。

1. コンフィグレーションの設定誤り
2. 本装置内の障害
3. ネームサーバの障害・設定誤り

本節では，障害部位および原因の切り分け手順を説明いたします。障害部位および原因の切り分け方法は，次のフローに従ってください。

(1)　ログおよびインタフェースの確認

通信ができなくなる原因として，ハードウェア（PRU ／ NIF ／ Line）の障害（または壊れ）や，隣接装置の障害が考えられます。本装置が表示するログや show ip interface コマンドによるインタフェースの up/down 状態を確認してください。手順については「8.5.1　通信ができない，または切断されている」を参照してください。

(2) 本装置の DNS リレー状態確認

(a) DNS リレーデーモンの起動確認

show dns-relay コマンドで DNS リレーデーモンから情報が取得できるか確認してください。show dns-relay コマンドの実行結果が次の場合は，コンフィグレーションコマンド dns-resolver でリレー機能を再設定してください。

［実行結果］

```
> show dns-relay
 Can not execute this command.
 No DNS relay configuration.
```

(b) ネームサーバの設定確認

show dns-relay コマンドで DNS リレーデーモンが使用しているネームサーバ情報を確認してください。ネームサーバが設定されていない場合は，コンフィグレーションの確認を参照してください。

```
>show dns-relay
 Primary   NameServer: 192.168.0.1
 Secondary NameServer: 192.168.0.2
 Thirdary  NameServer: -
 Error Statistics:
 Over max capacity   : 0
 Lack of memory      : 0
 Communication error : 0
 Communication status:
 <source IP address>   <destination IP address>   <status>
```


(c) DNS リレーの輻輳状態確認

DNS リレーは最大で 2000 個の要求を処理できます。しかし，その収容条件を超えてしまった場合は DNS リレーでクライアントへエラー応答を送信してしまいます。この状態に陥った要因を調査する場合は運用コマンドを使用して確認してください。

- 通信異常が発生している場合は，本装置からクライアント，およびネームサーバへのルーティングを確認してください。ネームサーバの確認は本項のネームサーバの確認に従ってください。
- 最大収容数オーバやメモリ不足が発生している場合は，クライアントからの要求が大量に発生していないか確認してください。
- 通信異常のリトライ処理により最大収容数オーバやメモリ不足が発生する場合もあります。最大収容数オーバやメモリ不足発生時は通信異常時の確認も実施してください。

```
>show dns-relay
 Primary   NameServer: 192.168.0.1
 Secondary NameServer: 192.168.0.2
 Thirdary  NameServer: -
 Error Statistics:
  Over max capacity   : 235 ←― 0以外は最大収容数オーバが発生しています
  Lack of memory      : 125 ←― 0以外はメモリー不足が発生しています
  Communication error : 374 ←― 0以外は通信エラーが発生しています
 Communication status:
  <source IP address>   <destination IP address>   <status>
  192.168.253.9         192.168.0.1                inquiry
  192.168.253.9         192.168.0.1                inquiry
  192.168.253.9         192.168.0.1                inquiry
  192.168.253.9         192.168.0.2                retry-inquiry(1)
  192.168.253.9         192.168.0.2                retry-inquiry(1)
       :                     :                          :
       :                     :                          :
  同一のIPアドレスからの大量アクセスがないか確認してください
```

(3) コンフィグレーションの確認

コンフィグレーションの誤りによって DNS リレーが通信を行えない可能性があります。次にコンフィグレーションの確認手順を示します。

(a) DNS リレー機能の有効設定確認

コンフィグレーションコマンド show dns-resolver で DNS リレー機能が有効になっているか確認してください。

```
>show dns-resolver
  dns_resolver yes {
   hostname router.mydomain.com;
   nameserver 192.168.0.1 ;
   nameserver 192.168.0.2 ;
   relay yes;  ←――― yesに設定されていることを確認してください
  };
```

(b) ネームサーバの設定確認

ネームサーバが設定されているか確認してください。

```
>show dns-resolver
 dns_resolver yes {
  hostname router.mydomain.com ;
   nameserver 192.168.0.1;  ←――― ネームサーバのIPアドレスが設定されていることを
   nameserver 192.168.0.2;       確認してください
 relay yes;
};
```

(4) ネームサーバの確認

本装置に異常が発生していなくても，ネームサーバがダウンしていたり，ルーティングできない IP アドレスが設定されていたりする場合には通信を行えません。ネームサーバに関連する情報の正常性や状態を確認してください。

(a) IP アドレスの正常性確認

コンフィグレーションコマンド dns-resolver で設定した IP アドレスに間違いがないか再度確認してくだ

さい。

(b) ネームサーバへのルーティング確認

コンフィグレーションコマンド dns-resolver で設定した IP アドレスと本装置の間で ping コマンドによる疎通試験を実施して，問題ないことを確認してください。

(c) ネームサーバの起動確認

ネームサーバ管理者にお問い合わせください。

8.6　IPv4 ユニキャストルーティングの通信障害

8.6.1　RIP 経路情報がない

本装置が取得した経路情報の表示に，RIP の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 8-19　RIP の障害解析方法

項番	確認内容・コマンド	対応
1	RIP の隣接情報を表示します。 show ip rip gateway	隣接ルータのインタフェースが表示されていない場合は項番 2 へ。
		隣接ルータのインタフェースが表示されている場合は項番 3 へ。
2	コンフィグレーションで RIP 定義が正しいか確認してください。	コンフィグレーションが正しい場合は項番 3 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
3	コンフィグレーションで経路フィルタリングが正しいか確認してください。	コンフィグレーションが正しい場合は項番 4 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
4	隣接ルータが RIP 経路を広告しているか確認してください。	広告している場合は該当ルータで障害情報を収集してください。 dump protocols unicast all ※
		広告していない場合は隣接ルータを確認してください。

注※　障害情報収集コマンドを実行すると，次に示すエリアにファイルが作成されます。
格納エリア：/primaryMC/var/rtm
ファイル名：rt_trace と rt_dump.gz

8.6.2　OSPF 経路情報がない

本装置が取得した経路情報の表示に，OSPF の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 8-20　OSPF の障害解析方法

項番	確認内容・コマンド	対応
1	OSPF のインタフェース状態を確認します。 show ip ospf interface <IP Address>	インタフェースの状態が DR または P to P の場合は項番 3 へ。
		インタフェースの状態が BackupDR または DR Other の場合は項番 2 へ。
		インタフェースの状態が Waiting の場合は，時間を置いてコマンド再投入してください。項番 1 へ。
2	Neighbor List より DR との隣接ルータ状態を確認します。	DR との隣接ルータ状態が Full 以外の場合は項番 4 へ。
		DR との隣接ルータ状態が Full の場合は項番 5 へ。
3	Neighbor List より全隣接ルータ状態を確認します。	一部の隣接ルータ状態が Full 以外の場合は項番 4 へ。

項番	確認内容・コマンド	対応
		全隣接ルータ状態が Full の場合は項番 5 へ。
4	コンフィグレーションで OSPF の定義が正しいか確認してください。	コンフィグレーションが正しい場合は項番 5 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
5	OSPF 経路を学習している経路を確認してください。 show ip route all-routes	経路が InActive または存在しない場合には項番 6 へ。
		経路が Active の場合は障害情報を収集してください。 dump protocols unicast all ※
6	コンフィグレーションでフィルタリングしていないか確認してください。	コンフィグレーションが正しい場合には項番 7 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
7	隣接ルータが OSPF 経路を広告しているか確認してください。	広告している場合は該当ルータで障害情報を収集してください。 dump protocols unicast all ※
		広告していない場合は隣接ルータを確認してください。

注※　障害情報収集コマンドを実行すると，次に示すエリアにファイルが作成されます。
格納エリア：/primaryMC/var/rtm
ファイル名：rt_trace と rt_dump.gz

8.6.3　BGP4 経路情報がない【OP-BGP】

本装置が取得した経路情報の表示に，BGP4 の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 8-21　BGP4 の障害解析方法

項番	確認内容・コマンド	対応
1	BGP4 のピア状態を確認します。 show ip bgp neighbor	ピア状態が Established 以外の場合は項番 2 へ。
		ピア状態が Established の場合は項番 3 へ。
2	コンフィグレーションで BGP4 の定義が正しいか確認してください。	コンフィグレーションが正しい場合は項番 3 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
3	BGP4 経路を学習しているか確認してください。 show ip bgp received-routes	経路が存在しない場合には項番 4 へ。
		経路が存在する場合は障害情報を収集してください。 dump protocols unicast all ※
4	コンフィグレーションでフィルタリングしていないか確認してください。	コンフィグレーションが正しい場合は項番 5 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
5	隣接ルータが BGP4 経路を広告しているか確認してください。	広告している場合は該当ルータで障害情報を収集してください。 dump protocols unicast all ※

項番	確認内容・コマンド	対応
		広告していない場合は隣接ルータを確認してください。

注※　障害情報収集コマンドを実行すると，次に示すエリアにファイルが作成されます。
格納エリア：/primaryMC/var/rtm
ファイル名：rt_trace と rt_dump.gz

8.6.4　IS-IS 経路情報がない【OP-ISIS】

本装置が取得した経路情報の表示に，IS-IS の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

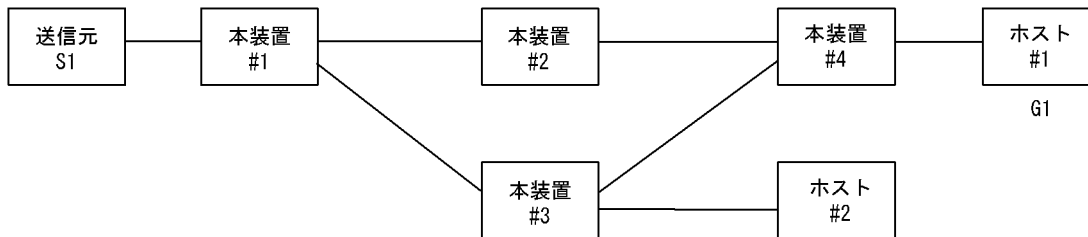
表 8-22　IS-IS の障害解析方法

項番	確認内容・コマンド	対応
1	IS-IS の隣接状態を確認します。 show isis adjacency	隣接状態が Up 以外の場合は項番 2 へ。
		隣接状態が Up の場合は項番 4 へ。
2	コンフィグレーションで IS-IS の定義が正しいか確認してください。	コンフィグレーションが正しい場合は項番 3 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
3	IS-IS のインタフェース状態を確認します。 show isis interface	インタフェース状態が Active の場合は項番 4 へ。
		インタフェース状態が Passive の場合は IS-IS 未サポートのインタフェースです。
4	IS-IS 経路を学習しているか確認してください。 show ip route all-routes	経路が InActive または存在しない場合には項番 5 へ。
		経路が Active の場合は障害情報を収集してください。dump protocols unicast all ※
5	コンフィグレーションでフィルタリングしていないか確認してください。	コンフィグレーションが正しい場合は項番 6 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
6	隣接ルータが IS-IS 経路を広告しているか確認してください。	広告している場合は該当ルータで障害情報を収集してください。dump protocols unicast all ※
		広告していない場合は隣接ルータを確認してください。

注※　障害情報収集コマンドを実行すると，次に示すエリアにファイルが作成されます。
格納エリア：/primaryMC/usr/var/rtm
ファイル名：rt_trace と rt_dump.gz

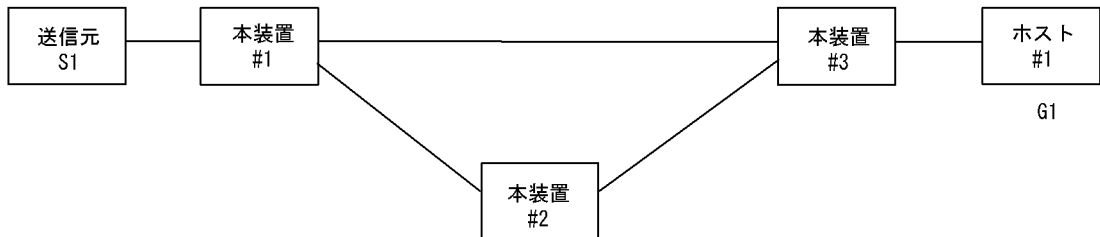
8.7 IPv4 マルチキャストルーティングの通信障害【OP-MLT】

本装置で IPv4 マルチキャスト通信ができない場合の対処について説明します。以下の対処を行う前に show pru resources コマンドでマルチキャスト通信できるリソース配分（例：router-b1）であることを確認してください。

8.7.1 PIM-DM ネットワークで通信ができない

本装置#2上の本装置#4とのIPアドレス < 本装置#3上の本装置#4とのIPアドレス

図に示す IPv4 PIM-DM ネットワークの構成で，送信元 S1 から G1 宛のパケットがホスト #1 で受信できない場合，次の手順に従って対処してください。

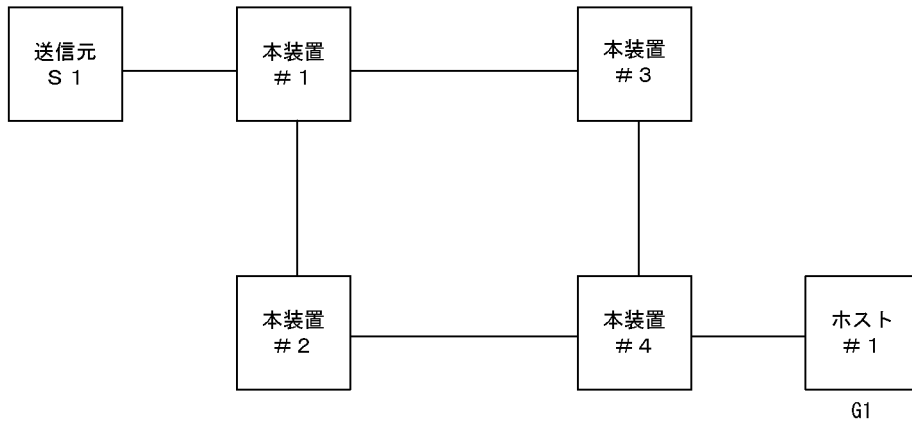
1. すべての本装置で show pru resources コマンドを実行し，PRU 上のハードウェアテーブルに IPv4 マルチキャスト経路を割り当ててあることを確認してください。
2. 本装置 #4 で show ip igmp interface コマンドを実行し，ホスト #1 とのインタフェースが enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
3. 本装置 #4 で show ip igmp groups コマンドを実行し，G1 グループにホスト #1 が参加していることを確認してください。
4. 本装置 #4 で show ip mcache コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュが存在していることを確認してください。存在しない場合は，本装置 #3 との PIM-DM のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
5. 本装置 #1 で show ip mcache コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュが存在していることを確認してください。存在しない場合は，S1 との PIM-DM のインタフェース定義が enable であり，フィルタなどによる抑止定義がないことを確認してください。
6. ルーティングキャッシュの下流が存在しない場合，show ip pim neighbor で本装置 #2 と本装置 #3 が表示されていることを確認してください。
7. 本装置 #3 で show ip mcache コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュが存在していることを確認してください。存在しない場合は，本装置 #1 との PIM-DM のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
8. ルーティングキャッシュの下流が存在しない場合，show ip pim neighbor で本装置 #1 と本装置 #4 が表示されていることを確認してください。
9. 本装置 #3 で show ip rpf [S1] コマンドを実行し，上流が本装置 #1 へのインタフェース，下流が本装置 #4 へのインタフェースを表示することを確認してください。

8.7.2 PIM-SM ネットワークで通信ができない

（1） PIM-SM ネットワーク

本装置#2はランデブーポイントおよびBSR

図に示す IPv4 PIM-SM ネットワークの構成で，IPv4 PIM-SM ネットワークで送信元 S1 から G1 宛のパケットがホスト #1 で受信できない場合，次の手順に従って対処してください。

1. すべての本装置で show pru resources コマンドを実行し，PRU 上のハードウェアテーブルに IPv4 マルチキャスト経路を割り当ててあることを確認してください。
2. すべての本装置のコンフィグレーションに SSM が定義されている場合は，G1 が SSM アドレスでないことを確認してください。
3. 本装置 #3 で show ip igmp interface コマンドを実行し，ホスト #1 とのインタフェースが enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
4. 本装置 #3 で show ip igmp groups コマンドを実行し，G1 グループにホスト #1 が参加していることを確認してください。
5. 本装置 #3 で show ip mroute コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュ（S,G）および G1 へのマルチキャストルーティングキャッシュ（*,G）が存在していることを確認してください。存在しない場合は，本装置と #1 および #2 との PIM-SM のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
6. 本装置 #1 で show ip mroute コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュが存在していることを確認してください。存在しない場合は，S1 との PIM-SM のインタフェース定義が enable であり，フィルタなどによる抑止定義がないことを確認してください。
7. ルーティングキャッシュの下流が存在しない場合，show ip pim neighbor で本装置 #2 と本装置 #3 が表示されていることを確認してください。また，ルーティングキャッシュが存在しない場合は，show ip pim bsr および show ip pim rendezvous-point mapping を実行し，BSR およびランデブーポイント（RP）が本装置 #2 であることを確認してください。
8. BSR およびランデブーポイント（RP）が存在しないか本装置 #2 でない場合，本装置 #2 で show ip pim bsr および show ip pim rendezvous-point mapping コマンドを実行し，本装置が BSR およびランデブーポイント（RP）であることを確認してください。本装置が BSR およびランデブーポイントでない場合，コンフィグレーションで BSR およびランデブーポイントの定義が正しいか確認してください。
9. 本装置 #2 で show ip mroute コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュ（S,G）および G1 へのマルチキャストルーティングキャッシュ（*,G）が存在していることを確認してください。存在しない場合は，本装置 #1 および本装置 #3 との PIM-SM のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
10. ルーティングキャッシュの下流が存在しない場合，show ip pim neighbor で本装置 #1 と本装置 #3 が表示されていることを確認してください。
11. ルーティングキャッシュが存在しない場合は，本装置 #3 で show ip pim bsr および show ip pim rendezvous-point mapping を実行し，BSR およびランデブーポイント（RP）が本装置 #2 であること

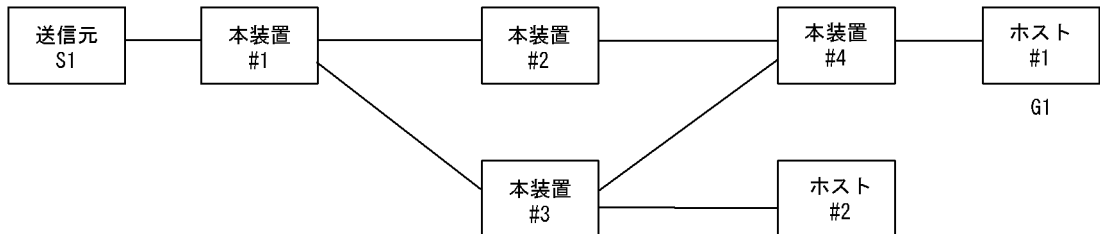
を確認してください。

（2） PIM-SSM ネットワーク

図に示す IPv4 PIM-SSM ネットワークの構成で，IPv4 PIM-SSM ネットワークで送信元 S1 から G1 宛のパケットがホスト #1 で受信できない場合，次の手順に従って対処してください。

1. すべての本装置で show pru resources コマンドを実行し，PRU 上のハードウェアテーブルに IPv4 マルチキャスト経路を割り当ててあることを確認してください。
2. すべての本装置のコンフィグレーションに SSM が定義され，G1 が SSM アドレスであることを確認してください。
3. 本装置 #4 で show ip igmp interface コマンドを実行し，ホスト #1 とのインタフェースが enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
4. 本装置 #4 で show ip igmp groups コマンドを実行し，G1 グループにホスト #1 が参加していることを確認してください。
5. 本装置 #4 で ssm-join のコンフィグレーションに（G1,S1）が定義されていることを確認してください。
6. 本装置 #4 で show ip rpf コマンドを実行し，S1 への経路を認識していることを確認してください（ここでは本装置 #2 側を上流とします)。
7. 本装置 #4 で show ip mroute コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュ（S1,G1）が存在していることを確認してください。存在する場合は，iif が装置 #2 側のインタフェースで，oif がホスト #1 側のインタフェースである SSM エントリであることを確認してください。存在しない場合は，本装置 #2 との PIM-SM のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
8. 本装置 #4 で show ip pim neighbor コマンドを実行し，本装置 #4 が本装置 #2 を認識できていることを確認してください。
9. 本装置 #2 で show ip mroute コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュ（S1,G1）が存在していることを確認してください。存在する場合は，iif が装置 #1 側のインタフェースで，oif が装置 #4 側のインタフェースである SSM エントリであることを確認してください。存在しない場合は，本装置 #4 および本装置 #1 との PIM-SM のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
10. 本装置 #2 で show ip pim neighbor コマンドを実行し，本装置 #2 が本装置 #4 および本装置 #1 を認識できていることを確認してください。
11. 本装置 #1 で show ip mroute コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュが存在していることを確認してください。存在する場合は，iif が S1 のインタフェースで，oif が装置 #2 側のインタフェースである SSM エントリであることを確認してください。存在しない場

合は，S1 との PIM-SM のインタフェース定義が enable であり，フィルタなどによる抑止定義がないことを確認してください。

12. 本装置 #1 で show ip pim neighbor コマンドを実行し，本装置 #1 が本装置 #2 を認識できていることを確認してください。

8.7.3 DVMRP ネットワークで通信ができない

本装置#2上の本装置#4とのIPアドレス ＜ 本装置#3上の本装置#4とのIPアドレス

図に示す IPv4 DVMRP ネットワークの構成で，送信元 S1 から G1 宛のパケットがホスト #1 で受信できない場合，次の手順に従って対処してください。

1. すべての本装置で show pru resources コマンドを実行し，PRU 上のハードウェアテーブルに IPv4 マルチキャスト経路を割り当ててあることを確認してください。
2. 本装置 #4 で show ip igmp interface コマンドを実行し，ホスト #1 とのインタフェースで IGMP と DVMRP のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。IGMP だけの定義では動作しません。
3. 本装置 #4 で show ip igmp groups コマンドを実行し，G1 グループにホスト #1 が参加していることを確認してください。
4. 本装置 #4 で show ip mcache コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュが存在していることを確認してください。存在しない場合は，本装置 #2 との DVMRP のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
5. 本装置 #1 で show ip mcache コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュが存在していることを確認してください。存在しない場合は，S1 との DVMRP のインタフェース定義が enable であり，フィルタなどによる抑止定義がないことを確認してください。
6. ルーティングキャッシュの下流が存在しない場合，show ip dvmrp neighbor で本装置 #2 と本装置 #3 が表示されていることを確認してください。
7. show ip dvmrp route [S1] コマンドを実行し，本装置 #2 か本装置 #3 へのルートが存在することを確認してください。ここで，本装置 #3 だけが表示された場合は本装置 #2 と本装置 #4 のインタフェースが障害でないか確認してください。
8. 本装置 #2 で show ip mcache コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュが存在していることを確認してください。存在しない場合は，本装置 #1 との DVMRP のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
9. ルーティングキャッシュの下流が存在しない場合，show ip dvmrp neighbor で本装置 #1 と本装置 #4 が表示されていることを確認してください。
10. 本装置 #2 で show ip dvmrp route [S1] コマンドを実行し，上流が本装置 #1 へのインタフェース，下流が本装置 #4 へのインタフェースを表示することを確認してください。

8.8　IPv6 ネットワークの通信障害

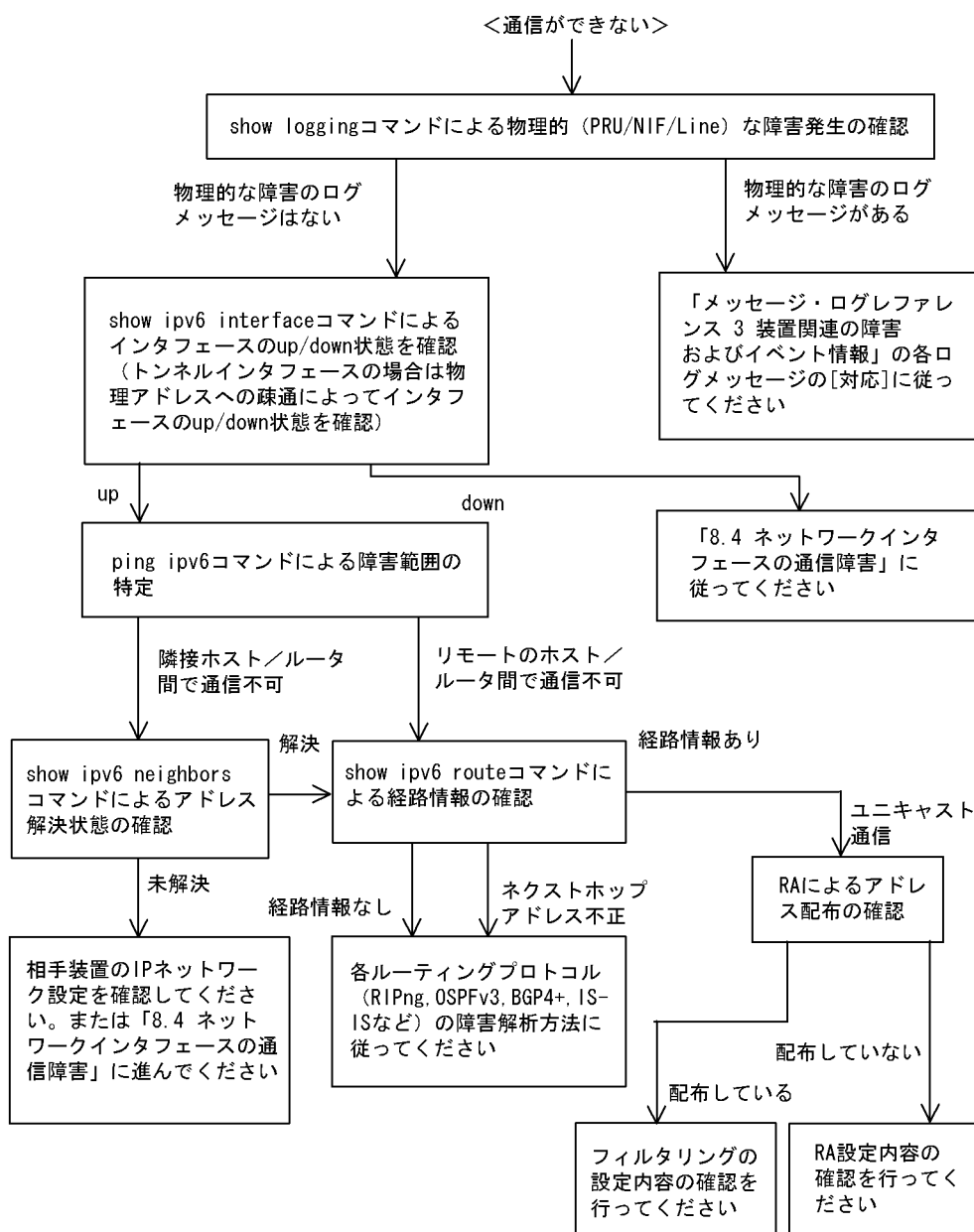
8.8.1　通信ができない，または切断されている

本装置を使用している IPv6 ネットワーク上で，通信トラブルが発生する要因として考えられるのは，次の 3 種類があります。

1. IPv6 通信に関係するコンフィグレーションの変更
2. ネットワークの構成変更
3. ネットワークを構成する機器の障害

上記 1. および 2. については，コンフィグレーションおよびネットワーク構成の変更前と変更後の差分を調べ，通信ができなくなるような原因がないか確認してください。

ここでは，3. に示すように「コンフィグレーションおよびネットワーク構成は正しいのに IPv6 通信ができない」，「これまで正常に動いていたのに IPv6 通信ができなくなった」というケースを中心に，障害部位および原因の切り分け手順を説明します。

障害部位および原因の切り分け方法は，次のフローに従ってください。

(1) ログおよびインタフェースの確認

通信ができなくなる原因として，ハードウェア（PRU ／ NIF ／ Line）の障害（または壊れ）や，隣接装置の障害が考えられます。本装置が表示するログや show ipv6 interface コマンドによるインタフェースの up/down 状態を確認してください。手順については，「8.5.1　通信ができない，または切断されている」を参照してください。

(2) 障害範囲の特定（本装置から実施する場合）

本装置に障害がない場合は，通信を行っていた相手との間のどこかに障害が発生している可能性があります。通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. 本装置にログインします。
2. ping ipv6 コマンドを使って通信できない両方の相手との疎通を確認してください。ping ipv6 コマンドの操作例および実行結果の見方は，「6.6.1　当該宛先アドレスとの通信可否を確認する」を参照してく

ださい)。

3. ping ipv6 コマンドで通信相手との疎通が確認できなかった場合は，さらに ping ipv6 コマンドを使って本装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping ipv6 コマンド実行の結果，障害範囲が隣接装置の場合は「(4) 隣接装置との NDP 解決情報の確認」に，リモート先の装置の場合は「(5) ユニキャストインタフェース情報の確認」に進んでください。

(3) 障害範囲の特定（お客様の端末装置から実施する場合）

本装置にログインできない環境にある場合に，お客様の端末装置から通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. お客様の端末装置に ping ipv6 機能があることを確認してください。
2. ping ipv6 機能を使って，お客様の端末装置と通信相手との疎通ができるか確認してください。
3. ping ipv6 機能で通信相手との疎通が確認できなかった場合は，さらに ping ipv6 コマンドを使ってお客様の端末装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping ipv6 機能による障害範囲が特定できたら，障害と考えられる装置が本装置である場合は本装置にログインして，障害解析フローに従って障害原因の調査を行ってください。

(4) 隣接装置との NDP 解決情報の確認

ping ipv6 コマンドの実行結果によって隣接装置との疎通が不可の場合は，NDP によるアドレスが解決していないことが考えられます。本装置と隣接装置間のアドレス解決状態を確認する手順を次に示します。

1. 本装置にログインします。
2. show ipv6 neighbors コマンドを使って隣接装置間とのアドレス解決状態（NDP エントリ情報の有無）を確認してください。
3. 隣接装置間とのアドレスが解決している（NDP エントリ情報あり）場合は，「(5) ユニキャストインタフェース情報の確認」に進んでください。
4. 隣接装置間とのアドレスが解決していない（NDP エントリ情報なし）場合は，隣接装置と本装置の IP ネットワーク設定が一致しているかを確認してください。

(5) ユニキャストインタフェース情報の確認

隣接装置とのアドレスが解決しているにもかかわらず通信ができない場合や，IPv6 ユニキャスト通信で通信相手との途中の経路で疎通が不可となる，または通信相手までの経路がおかしいなどの場合は，本装置が取得した経路情報を確認する必要があります。確認手順を次に示します。

1. 本装置にログインします。
2. show ipv6 route コマンドを実行して，本装置が取得した経路情報を確認してください。
3. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がない場合やネクストホップアドレスが不正の場合は「8.9 IPv6 ユニキャストルーティングの通信障害」に進んでください。
4. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がある場合は，通信不可のインタフェースに設定している次の機能に問題があると考えられます。該当する機能の調査を行ってください。
   - RA 機能
     「(7) RA 設定情報の確認」に進んでください。
   - トンネルインタフェース
     「(11) トンネルインタフェース設定情報の確認」に進んでください。

(6) フィルタリング／ QoS 設定情報の確認

本装置において，物理的障害がなく，経路情報も正しく設定されているにもかかわらず通信ができない場合は，フィルタリング機能により特定のパケットだけを廃棄する設定になっているか，QoS 機能の帯域制御または優先廃棄制御によりパケットが廃棄されている可能性があります。

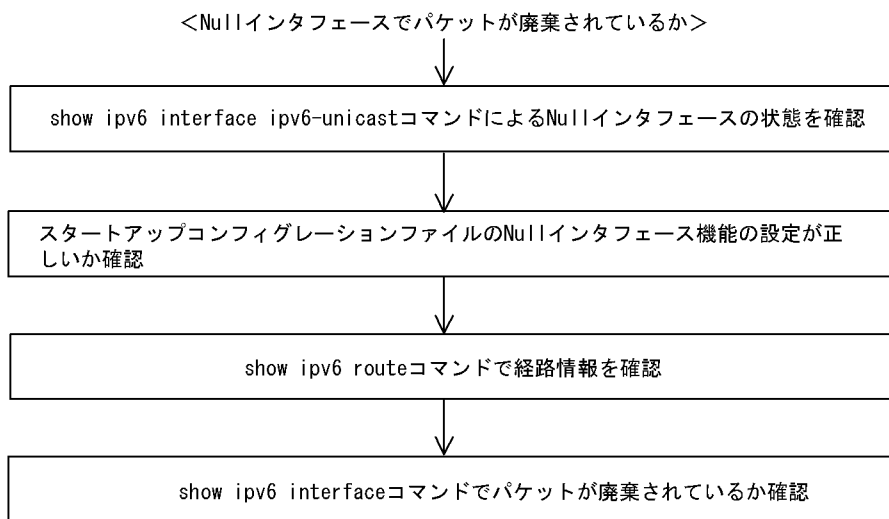
したがって，コンフィグレーションのフィルタリング機能および QoS 機能の設定条件が正しいか，システムの構築において帯域制御ならびに優先廃棄制御がシステム運用において適切であるか見直してください。手順については，「8.5.1　通信ができない，または切断されている　(7) フィルタリング／ QoS 設定情報の確認」を参照してください。

(7) RA 設定情報の確認

本装置と本装置に直接接続されている端末との間で通信ができない場合は，RA によるアドレス情報配布が正常に行われていない可能性が考えられます。したがって，コンフィグレーションの RA 機能の設定が正しいか確認してください。手順については「6.7.6　IPv6 アドレス情報が正しく配布されているかを確認する」を参照してください。IPv6 アドレス情報が正しく配布されていた場合，通信不可のインタフェースに設定している次の機能に問題があると考えられます。該当する機能の調査を行ってください。

- フィルタリング／ QoS 機能
  「(6) フィルタリング／ QoS 設定情報の確認」を参照してください。

(8) Null インタフェース設定情報の確認

特定のネットワーク宛または特定の端末宛の通信を Null インタフェースに向けて制限しているにもかかわらず，パケットが廃棄されない場合は，Null インタフェースの設定内容に誤りがある可能性があります。次の手順で Null インタフェースの設定内容が正しいか確認してください。

1. show ipv6 interface ipv6-unicast コマンドを使い Null インタフェースの状態を確認します。Null インタフェースが UP しているか確認してください。
2. スタートアップコンフィグレーションファイルで Null インタフェースが定義されているか確認します。
3. show ipv6 route コマンドで経路情報を確認します。
   static コマンドで定義した経路情報の設定内容が正しいか確認してください。
4. パケットが廃棄されているか確認します。
   show ip interface コマンドを使って Null インタフェースでパケットが廃棄されているか確認してくだ

さい。

(9) ポリシールーティング設定情報の確認

本装置において物理的障害は発生してなく，経路情報も正しく設定されているにもかかわらず通信ができない場合は，ポリシールーティング機能の出力先インタフェースに障害が発生しているためにパケットが廃棄されている可能性が考えられます。

したがって，次の手順でポリシールーティングの現在使用されている出力先インタフェースの状態を確認してください。

(a) ポリシールーティング機能による出力先インタフェースの確認方法

1. 本装置にログインします。
2. show ipv6 policy コマンドを使って，入力インタフェースのポリシールーティング設定内容と，現在使用されている出力先インタフェースの状態を確認します。

［確認例］

通信できないパケットの入力インタフェースが tokyo，送信元 IP アドレスが 3ffe:101::105 の場合に，ポリシールーティング機能で使用されている出力先を確認します。

1. 本装置にログインします。
2. 「show ipv6 policy interface tokyo」と入力します。

```
> show ipv6 policy interface tokyo
<Interface Name>            <Filter List No>
  tokyo                      40001,40002
>
```

3. 入力インタフェース tokyo で使用されている条件番号を確認します。
上記例では，＜ Filter List No. ＞:40001,40002 が該当します。
4. 3. で確認した条件の詳細を表示します。「show ipv6 local policy interface tokyo 40001 40002」と入力します。

```
> show ipv6 policy policy interface tokyo 40001 40002
<Interface Name>: tokyo           <Filter List No.> 40001
        forward packets
        protocol                  : ip
        ip_source                 : 3ffe:101::101 - 3ffe:101::1ff
        ip_destination            : 3ffe:201::101 - 3ffe:201::1ff
        current policy route
          Policy Group Name         v6route1
          Output Interface          tokyo3
          Next Hop IP address       3ffe:c01::2
<Interface Name>: tokyo           <Filter List No.> 40002
        forward packets
        protocol                  : ip
        ip_source                 : 3ffe:401::201 - 3ffe:401::2ff
        ip_destination            : 3ffe:501::201 - 3ffe:501::2ff
        current policy route
          Policy Group Name         v6route2
          Output Interface          yokohama
          Next Hop IP address       3ffe:601::2
>
```

5. 各条件の内容と条件とその際の出力先を確認します。
通信できないパケットの内容を比較して，一致する条件のポリシールーティンググループ名称を確認します。
6. 採用されているポリシーグループの状態を確認します。「show ipv6 cache policy route1」と入力します。

```
> show ipv6 cache policy route1
<Policy Group Name>:     route1
       priority  Interface Name  status   Nexthop
           1     tokyo1            Down   3ffe:a01::2
           2     tokyo1            Down   3ffe:a11::2
           3     tokyo2            Down   3ffe:b01::2
   *>      4     tokyo3            Down   3ffe:c01::2    default
>
```

7. 出力先インタフェースが障害により出力できないためパケットが廃棄されています。スタートアップコンフィグレーションファイルのポリシー情報の設定を見直すと共に，「8.4　ネットワークインタフェースの通信障害」に従ってください。
   なお，show ipv6 cache policy コマンド実行時，使用中の経路がない（経路の先頭に *> の表示がない）場合も，出力先インタフェースの障害によりパケットが廃棄されていることを表します。

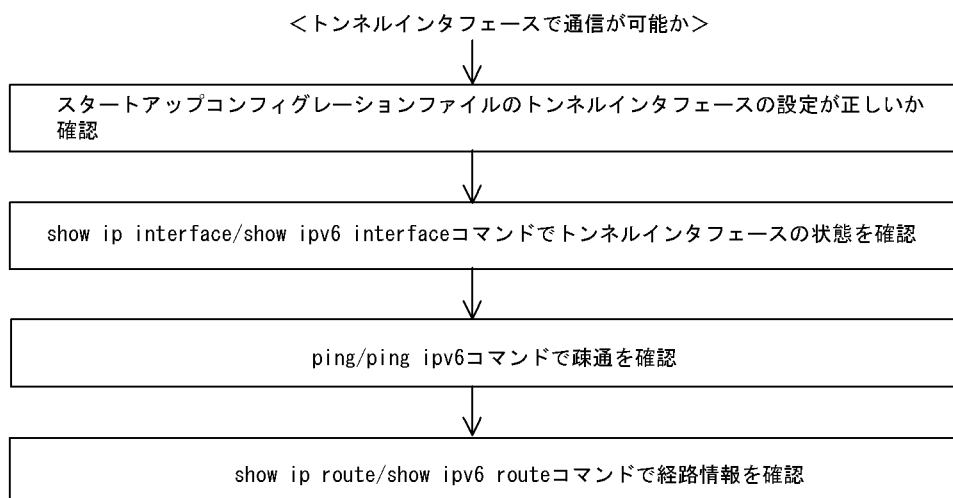
（10）Tag-VLAN 連携設定情報の確認

本装置に，IP インタフェース情報，経路情報が正しく設定されているにもかかわらず通信ができない場合は，Tag-VLAN 連携情報の設定が誤っている（またはされていない）ために，パケットが廃棄されている可能性が考えられます。本装置の Tag-VLAN 連携設定情報を確認する手順を次に示します。

1. 本装置にログインします。
2. show interfaces コマンドを使用して Tag-VLAN 連携設定情報（VLAN エントリ情報の有無，VLAN ID）を確認してください。
3. Tag-VLAN 連携設定情報が正しい（VLAN エントリ情報あり，正しい VLAN ID）場合は，show interfaces コマンドを使用して Tag-VLAN 連携設定情報（Tag-VLAN 連携設定の有無）を確認してください。

上記コマンドで Tag-VLAN 連携の設定が正しいと確認できた場合は，本装置に関する Tag-VLAN 連携の設定に問題はありません。接続装置（LAN Switch など）の設定に問題（VLAN 設定をしていない，VLAN ID が一致していない）がある可能性があるで，接続装置の設定情報を確認してください。

（11）トンネルインタフェース設定情報の確認

本装置にトンネルインタフェースを設定している状態で，特定のネットワーク宛または特定の端末宛の通信ができない場合，トンネルインタフェースの設定内容／ネットワーク構成に誤りがある可能性があります。次の手順でトンネルインタフェースの設定内容／ネットワーク構成が正しいか確認してください。

1. コンフィグレーションでトンネルインタフェースの定義を確認します。
   - コンフィグレーションコマンド tunnel（「コンフィグレーションコマンドレファレンス Vol.1 tunnel（トンネル情報）」を参照）で設定したトンネル情報のアドレスが，本装置のトンネルインタフェース以外のインタフェースに設定されていることを確認してください。アドレスが間違っている場合，正しいアドレスに変更してください。
   - トンネル情報に設定したアドレスと，コンフィグレーションコマンドの ip でトンネルインタフェースに設定したアドレスのプロトコルが同一でないことを確認してください。同一の場合は，正しいアドレスに変更してください。
2. show ipv6 interface コマンドを使用して，トンネルインタフェースの状態を確認します。
   - 表示結果の physical address で示すアドレスが，本装置のトンネルインタフェース以外のインタフェースに設定されているアドレスであることを確認してください。アドレスが間違っている場合には，正しいアドレスに変更してください。
   - 表示結果の physical address で示すアドレスが設定されているインタフェースの状態が，UP しているか確認してください。状態が UP となっていない場合は，当該インタフェースの障害と考えられます。「8.5.1　通信ができない，または切断されている」または「8.8.1　通信ができない，または切断されている」を参照してください。
3. トンネル情報で設定した自アドレス・宛先アドレスに対して，本装置および接続先装置より ping, ping ipv6 コマンドを使用して到達性を確認します。
   - どちらの装置からも到達性がない場合は，経路情報に問題があると考えられます。「8.5.1　通信ができない，または切断されている」または「8.8.1　通信ができない，または切断されている」を参照してください。
   - 一方の装置から到達性がない場合は，中継経路間にアドレス変換装置がないかネットワーク構成を確認してください。アドレス変換装置を使用している場合は禁止構成に該当するので，トンネルを設定する中継経路間にアドレス変換装置を設置しないようにネットワーク構成を変更してください（禁止構成については「解説書 Vol.1　12.11.4 トンネル機能使用時の注意事項」を参照してください）。
4. ネットワーク構成を確認します。
   - トンネルインタフェースに設定した接続先アドレスの到達経路を，show netstat routing-table numeric コマンドを使用して確認してください。経路の中継先が，本装置の別のトンネルインタフェースであった場合，禁止構成である多重トンネルとなっていることが考えられます。経路制御の設定を変更して，トンネルインタフェース以外が中継先となるように変更してください（禁止構成については「解説書 Vol.1　12.11.4 トンネル機能使用時の注意事項」を参照してください）。

8.8.2　IPv6 DHCP に関するトラブルシューティング

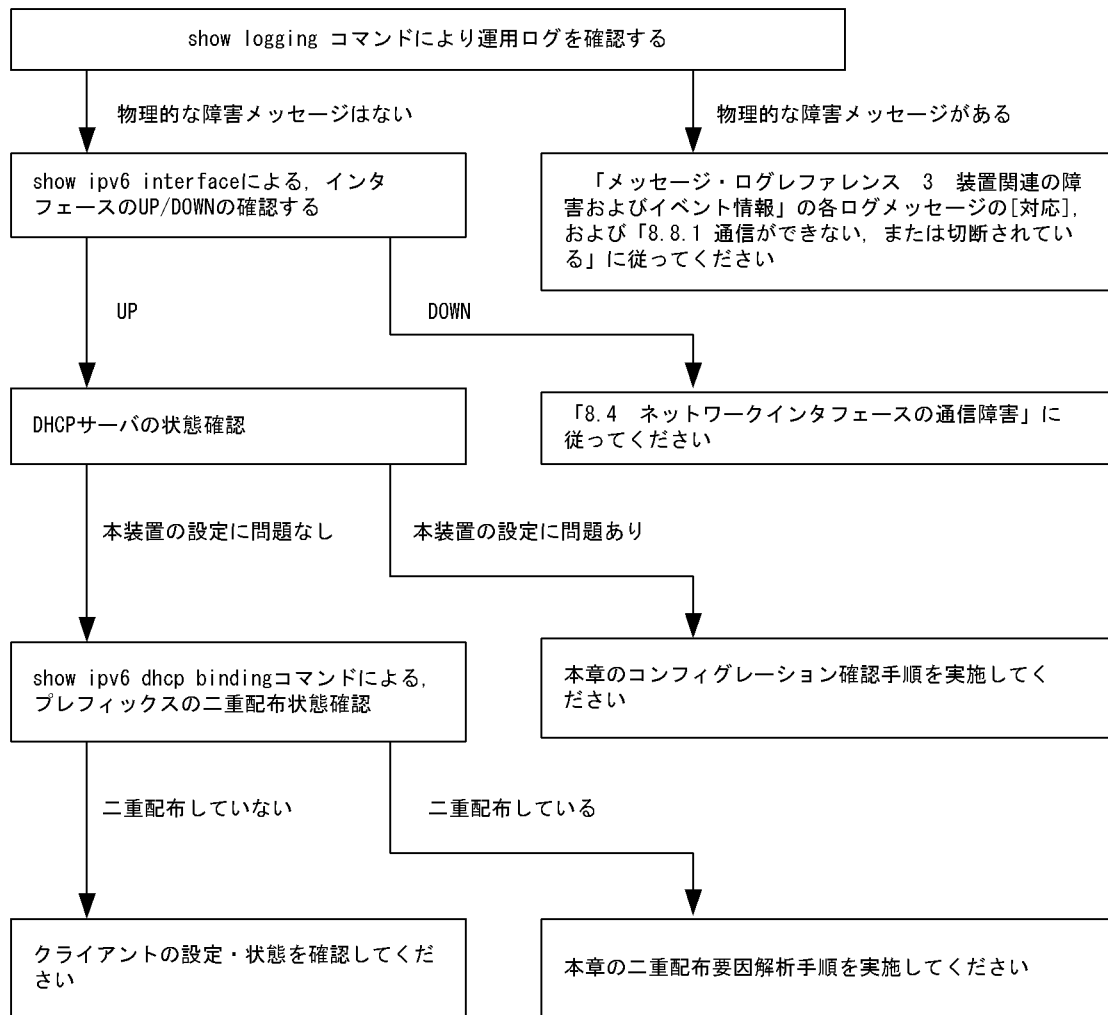
(1) コンフィグレーションが配布されない

本装置 DHCP サーバのプレフィックス配布機能を使用するに当たり，サービスが正常に動作しない原因としては，以下の 5 点が考えられます。

1. プレフィックス配布定義数に対して，クライアント数が多い。
2. クライアント DUID（DHCP Unique Identifier）の指定を誤っている。
3. dhcp6-server interface 定義を誤っている。
4. DHCP 運用中の障害
5. その他の障害

上記は，以下の手順で障害個所を切り分け，確認できます。

図 8-7 DHCP サーバの障害解析手順

<コンフィグレーションが配布できない>

(a) ログおよびインタフェースの確認

通信ができなくなる原因として，ハードウェア (PRU ／ NIF ／ Line) の障害 (または壊れ) や，隣接装置の障害が考えられます。本装置が表示するログや，show ipv6 interface コマンドによるインタフェースの up/down 状態を確認してください。手順については「8.8.1 通信ができない，または切断されている」を参照してください。

(b) 本装置の DHCP サーバ状態確認

1. DHCP サーバサービスの起動確認
   show ipv6 dhcp server statistics コマンドで，DHCP サーバデーモンから情報が取得できるか確認してください。show ipv6 dhcp server statistics コマンドの実行結果が下記の場合は，コンフィグレーションコマンド dhcp6-server で DHCP サーバ機能を再設定してください。

   [実行結果]

```
> show ipv6 dhcp server statistics
> < show statistics >: dhcp6_server doesn't seem to be running.
```

2. 配布可能なプレフィックスの残数を確認する

show ipv6 dhcp server statistics コマンドで，DHCP サーバがあといくつプレフィックスを配布できるかを確認してください。確認手順は「6.6.8　IPv6 DHCP サーバ機能を確認する　(2) 運用中の確認」を実施してください。確認の結果，配布可能なプレフィックス数が 0 である場合は配布するプレフィックス数を増やしてください。なお，配布可能なプレフィックス数の上限は 8192 です。

(c) コンフィグレーション確認手順

1. DHCP サーバ機能の有効設定の確認
   コンフィグレーションコマンド show dhcp6-server コマンドで，DHCP サーバ定義が有効になっているかを確認してください。実行結果で示す下線部が，no ではなく yes であれば，定義は有効です。

   [実行結果]

```
(config)# show dhcp6-server
dhcp6-server yes
!
(config)#
```

2. インタフェース (dhcp6-server interface) 定義を確認する
   コンフィグレーションコマンド show dhcp6-server interface コマンドで，DHCP サーバインタフェース定義の有無を確認してください。定義がない場合は追加してください。定義がある場合は，定義しているインタフェースが，クライアント接続ネットワーク向けの定義であるかを確認してください。

   [実行結果]

```
(config)# show dhcp6-server interface
dhcp6-server yes
dhcp6-server interface TokyoOsaka
  preference 100
!
(config)#
```

3. ホスト (dhcp6-server host) 定義を確認する
   コンフィグレーションコマンド show dhcp6-server host コマンドで，DHCP サーバで配布しようとしているプレフィックス配布定義の有無を確認してください。定義がない場合は追加してください。定義がある場合は，配布するプレフィックスを指定する prefix ／ range の設定値，配布クライアントを決める duid の定義有無，ならびに duid に指定したクライアント DUID の値が正しいかを確認してください。

   [実行結果]

```
(config)# show dhcp6-server host Tokyo1
dhcp6-server yes
dhcp6-server host Tokyo1
  duid any
  range 3ffe:ffff:1111::/48 3ffe:ffff:1112::/48
!
(config)#
```

4. ホストターゲット (dhcp6-server host-target) の確認
   本装置 DHCP サーバは，コンフィグレーションコマンド dhcp6-server interface の host-target にホスト定義名を指定することで，クライアントが接続されるネットワークを制限できます。そのため，host-target を指定するインタフェースを誤ると，その他のインタフェースで目的のクライアントから要求を受信した場合に，要求を廃棄します。DHCP サーバのコンフィグレーションを見直し，host-target を指定しているインタフェースや，指定しているホスト定義名の指定が正しいかどうかの確認を行ってください。

   [実行結果]

```
(config)# show dhcp6-server interface
dhcp6-server yes
dhcp6-server interface TokyoOsaka
  preference 100
  host-target Osaka
```

```
  host-target Tokyo
!
(config)#
```

(d) クライアントによる二重取得

1. binding 情報の確認

   show ipv6 dhcp binding detail コマンドにより，同一 DUID に対してプレフィックスが二重で配布されていないかを確認します。以下に表示例を示します。

   [実行結果]

```
> show ipv6 dhcp binding detail
Total: 2 prefixes
<Prefix>              <Lease expiration>  <Type>
  <DUID>
3ffe:1234:5678::/48      03/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
3ffe:aaaa:1234::/48      03/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
>
```

   下線で示すように，同一 DUID が 2 個以上存在する場合は，プレフィックス情報を不当に取得しているクライアントである可能性があります。各クライアントを確認し，配布を受けたプレフィックス値を確認してください。

2. 配布済みプレフィックスとクライアントの対応をとる

   show ipv6 dhcp binding detail の結果において，プレフィックスを二重取得しているクライアントが見つからない場合は，表示される DUID とクライアント装置の対応を取る手順が必要となります。対応付けは，binding 情報に示される「配布済みプレフィックスの値」と「クライアント装置が配布を受けたプレフィックスの情報」を比較することで確認してください。

(e) クライアントの設定状態を確認する

クライアントの設定状態を確認する場合は，クライアント付属のマニュアルに従ってください。

(f) 二重配布からの回復手順

本装置 DHCP サーバで，同一クライアントへプレフィックスを二重配布したことを確認した場合は，表示される DUID とクライアントの対応から，現在未使用のプレフィックスを調査してください。現在未使用のプレフィックスについては，clear ipv6 dhcp binding < 未使用プレフィックス > コマンドによって，binding 情報を削除してください。

[実行結果]

```
> show ipv6 dhcp binding detail
Total: 2 prefixes
<Prefix>              <Lease expiration>  <Type>
  <DUID>
3ffe:1234:5678::/48      03/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
3ffe:aaaa:1234::/48      03/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
> clear ipv6 dhcp binding 3ffe:1234:5678::/48
> show ipv6 dhcp binding detail
<Prefix>              <Lease expiration>  <Type>
  <DUID>
3ffe:aaaa:1234::/48      03/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
>
```

(2) プレフィックス配布先への通信ができない

本装置 DHCP サーバのプレフィックス配布先への自動経路情報設定機能を利用する場合，経路情報が設定されない要因は以下の二つがあります。

1. コンフィグレーション済みだが，未配布である。
2. 自動経路情報設定に関連する機能に影響がある操作，またはイベントが発生した。

上記は経路情報を確認する show ipv6 route -s コマンドの結果と show ipv6 dhcp server binding コマンドでの配布済みプレフィックス情報を比較することで切り分けることができます。

表 8-23 プレフィックス配布先への経路情報関連障害切り分け

条件		発生要因
binding 情報	経路情報	
有	経路あり	該当なし。正常運用状態。
有	経路なし	要因 2
無	経路あり	要因 2
無	経路なし	要因 1，2

プレフィックス配布先への経路情報の保有性については，次の表に示す制限があります。

表 8-24 プレフィックス配布先への経路情報の保有性

保有情報	発生イベントと保有性			
	サーバ機能再起動	ルーティングマネージャ再起動	本装置再起動	BCU 二重化切り替え
クライアントへの経路情報	○	○	×	△

（凡例）
○：保証される
△：保証される。ただし，一部，BCU 切り替え直前に配布したものについては保証されません
×：削除される (再設定要)

注
プレフィックス配布先への経路情報設定を行う際に必要な経路管理機能
なお，その他の障害については，「8.8.1 通信ができない，または切断されている」を参照してください。

(a) 経路情報の確認

本装置 DHCP サーバのプレフィックス配布先への自動経路設定機能を利用する場合，プレフィックス配布後の経路情報は，経路情報を確認する show ipv6 route -s コマンドで確認できます。

図 8-8 運用コマンドによる経路情報の確認

```
> show ipv6 route -s
Total: 10routes
Destination              Next Hop       Interface        Metric  Protocol  Age
3ffe:1234:5678::/48      ::1            tokyo            0/0      Static   45m
        <Active Gateway Dhcp>
3ffe:aaaa:1234::/48      ::1            osaka            0/0      Static   23m
        <Active Gateway Dhcp>
 :
>
```

(b) 経路情報の再設定を行う

本装置 DHCP サーバのプレフィックス配布先への自動経路設定機能を利用する場合，障害などで経路情報がクリアされるイベントが発生したとき，その復旧にはプレフィックスの再配布が必要です。クライアント装置で，プレフィックス情報を再取得する操作を行ってください。

（3） 本装置 DUID が他装置と重複した場合

本装置を含む DHCP サーバを同一ネットワーク上で 2 台以上運用する構成で，DUID が重複する場合は，下記手順で本装置の DUID を再設定してください。

（a） DUID 情報保存ファイルを削除する

本装置 DUID は /primaryMC/usr/var/dhcp6/dhcp6s_duid に保存されています。運用コマンドラインより，rm コマンドを使用し，明示的に削除してください。

（b） DUID を再生成させる

DUID ファイルを削除後は，restart ipv6-dhcp server コマンドによって再起動させるか，コンフィグレーションへ DHCPv6 サーバ定義を追加してください。本装置 DHCP サーバは起動時に DHCP インタフェースとして使用する ipv6 インタフェースの MAC アドレスを取得し，これと時刻情報を基に新たに生成します。

（c） DUID の確認

show ipv6 dhcp server statistics コマンドによって確認できます。詳細は「6.6.8　IPv6 DHCP サーバ機能を確認する　（4）DUID(DHCP Unique Identifier) について」を参照してください。

8.8.3 トンネルインタフェース上で通信ができない

通信障害の原因がトンネル回線にあると考えられる場合は，以下に従い確認をしてください。

（1） 状態確認

show interfaces コマンドにより，該当するトンネル回線状態を確認します。表示されるトンネル回線状態を次の表のとおり確認します。

表 8-25　トンネル回線状態の確認／対応

項番	Line 状態	原因	対応
1	active up	当該トンネル回線は正常に動作中です。	なし。
2	active down	当該トンネル回線に回線障害が発生しています。	当該トンネル回線が 6to4 トンネルの場合だけ発生する状態です。show logging コマンドにより表示される当該 6to4 トンネル回線に対応する回線のログより，「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」の該当メッセージを参照し，記載されている［対応］に従って対応してください。
3	locked	コンフィグレーションにより当該トンネルの運用が停止されています。	コンフィグレーションを設定して当該トンネルを運用状態にしてください。

（2） 統計情報の確認

show interfaces コマンドにより，当該トンネル回線の統計情報（パケット受信・送信失敗）を確認してください。パケット受信・送信失敗が発生している場合は，「8.8.1　通信ができない，または切断されている　（11）トンネルインタフェース設定情報の確認」に従って設定情報の確認をしてください。

8.9 IPv6 ユニキャストルーティングの通信障害

8.9.1 RIPng 経路情報がない

本装置が取得した経路情報の表示に，RIPng の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 8-26 RIPng の障害解析方法

項番	確認内容・コマンド	対応
1	RIPng の隣接情報を表示します。 show ipv6 rip gateway	隣接ルータのインタフェースが表示されていない場合は項番 2 へ。
		隣接ルータのインタフェースが表示されている場合は項番 3 へ。
2	コンフィグレーションで RIPng 定義が正しいか確認してください。	コンフィグレーションが正しい場合は項番 3 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
3	コンフィグレーションで経路フィルタリングが正しいか確認してください。	コンフィグレーションが正しい場合は項番 4 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
4	隣接ルータが RIPng 経路を広告しているか確認してください。	広告している場合は該当ルータで障害情報を収集してください。 dump protocols unicast all ※
		広告していない場合は隣接ルータを確認してください。

注※ 障害情報収集コマンドを実行すると，次に示すエリアにファイルが作成されます。
格納エリア：/primaryMC/var/rtm
ファイル名：rt_trace と rt_dump.gz

8.9.2 OSPFv3 経路情報がない

本装置が取得した経路情報の表示に，OSPFv3 の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 8-27 OSPFv3 の障害解析方法

項番	確認内容・コマンド	対応
1	OSPFv3 のインタフェース状態を確認します。 show ipv6 ospf interface <Interface Name>	インタフェース状態が DR または P to P の場合は項番 3 へ。
		インタフェース状態が BackupDR または DR Other の場合は項番 2 へ。
		インタフェースの状態が Waiting の場合は，時間を置いてコマンド再投入してください。項番 1 へ。
2	Neighbor List 内より DR との隣接ルータ状態を確認します。	DR との隣接ルータ状態が Full 以外の場合は項番 4 へ。
		DR との隣接ルータ状態が Full の場合は項番 5 へ。

項番	確認内容・コマンド	対応
3	Neighbor List 内より全隣接ルータとの状態を確認します。	一部の隣接ルータ状態が Full 以外の場合は項番 4 へ。
		全隣接ルータ状態が Full の場合は項番 5 へ。
4	コンフィグレーションで OSPFv3 の定義が正しいか確認してください。	コンフィグレーションが正しい場合は項番 5 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
5	OSPFv3 経路を学習している経路を確認してください。 show ipv6 route all-routes	経路が InActive または存在しない場合には項番 6 へ。
		経路が存在する場合は障害情報を収集してください。 dump protocols unicast all※
6	コンフィグレーションでフィルタリングしていないか確認してください。	コンフィグレーションが正しい場合は項番 7 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
7	隣接ルータが OSPFv3 経路を広告しているか確認してください。	広告している場合は該当ルータで障害情報を収集してください。 dump protocols unicast all※
		広告していない場合は隣接ルータを確認してください。

注※　障害情報収集コマンドを実行すると，次に示すエリアにファイルが作成されます。
格納エリア：/primaryMC/var/rtm
ファイル名：rt_trace と rt_dump.gz

8.9.3　BGP4+ 経路情報がない【OP-BGP】

本装置が取得した経路情報の表示に，BGP4+ の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 8-28　BGP4+ の障害解析方法

項番	確認内容・コマンド	対応
1	BGP4+ のピア状態を確認します。 show ipv6 bgp neighbor	ピア状態が Established 以外の場合は項番 2 へ。
		ピア状態が Established の場合は項番 3 へ。
2	コンフィグレーションで BGP4+ の定義が正しいか確認してください。	コンフィグレーションが正しい場合は項番 3 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
3	BGP4+ 経路を学習しているか確認してください。 show ipv6 bgp received-routes	経路が存在しない場合には項番 4 へ。
		経路が存在する場合は障害情報を収集してください。 dump protocols unicast all※
4	コンフィグレーションでフィルタリングしていないか確認してください。	コンフィグレーションが正しい場合は項番 5 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。

項番	確認内容・コマンド	対応
5	隣接ルータが BGP4+ 経路を広告しているか確認してください。	広告している場合は該当ルータで障害情報を収集してください。 dump protocols unicast all ※
		広告していない場合は隣接ルータを確認してください。

注※　障害情報収集コマンドを実行すると，次に示すエリアにファイルが作成されます。
格納エリア：/primaryMC/var/rtm
ファイル名：rt_trace と rt_dump.gz

8.9.4　IS-IS 経路情報がない【OP-ISIS】

本装置が取得した経路情報の表示に，IS-IS の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

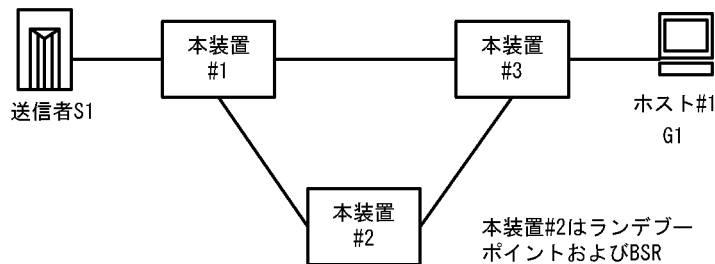
表 8-29　IS-IS の障害解析方法

項番	確認内容・コマンド	対応
1	IS-IS の隣接状態を確認します。 show isis adjacency	隣接状態が Up 以外の場合は項番 2 へ。
		隣接状態が Up の場合は項番 4 へ。
2	コンフィグレーションで IS-IS の定義が正しいか確認してください。	コンフィグレーションが正しい場合は項番 3 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
3	IS-IS のインタフェース状態を確認します。 show isis interface	インタフェース状態が Active の場合は項番 4 へ。
		インタフェース状態が Passive の場合は IS-IS 未サポートのインタフェースです。
4	IS-IS 経路を学習しているか確認してください。 show ipv6 route all-routes	経路が InActive または存在しない場合には項番 5 へ。
		経路が Active の場合は障害情報を収集してください。dump protocols unicast all ※
5	コンフィグレーションでフィルタリングしていないか確認してください。	コンフィグレーションが正しい場合は項番 6 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
6	隣接ルータが IS-IS 経路を広告しているか確認してください。	広告している場合は該当ルータで障害情報を収集してください。 dump protocols unicast all ※
		広告していない場合は隣接ルータを確認してください。

注※　障害情報収集コマンドを実行すると，次に示すエリアにファイルが作成されます。
格納エリア：/primaryMC/usr/var/rtm
ファイル名：rt_trace と rt_dump.gz

8.10 IPv6 マルチキャストルーティングの通信障害【OP-MLT】

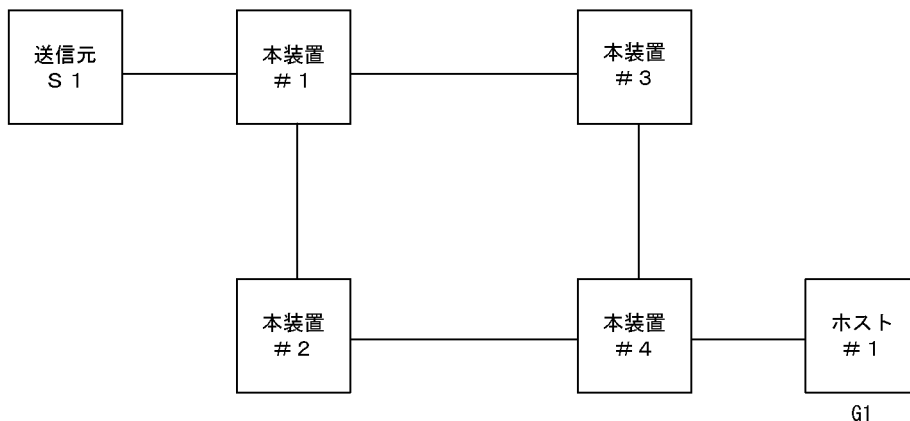
本装置で IPv6 マルチキャスト通信ができない場合の対処について説明します。以下の対処を行う前に show pru resources コマンドでマルチキャスト通信できるリソース配分（例：router-b1）であることを確認してください。

8.10.1 PIM-SM ネットワークで通信ができない

（1） PIM-SM ネットワーク

図に示す IPv6 PIM-SM ネットワークの構成で，送信元 S1 から G1 宛のパケットがホスト #1 で受信できない場合，次の手順に従って対処してください。

1. すべての本装置で show pru resources コマンドを実行し，PRU 上のハードウェアテーブルに IPv6 マルチキャスト経路を割り当ててあることを確認してください。
2. 本装置 #3 で show ipv6 mld interface コマンドを実行し，ホスト #1 とのインタフェースが表示されること，QoS 制御などによる中継抑止定義がないことを確認してください。
3. 本装置 #3 で show ipv6 mld group コマンドを実行し，G1 グループにホスト #1 が参加していることを確認してください。
4. 対ホストインタフェースの MLD バージョンを確認し，ホストの MLD パケットが受信できる状態であることを確認してください。
5. 本装置 #3 で show ipv6 mroute コマンドを実行し，送信元 S1 から G1 への IPv6 マルチキャストルーティングテーブル（S1,G1）および G1 への IPv6 マルチキャストルーティングテーブル（*,G1）が存在していることを確認してください。存在しない場合は，本装置と #1 および #2 との IPv6 PIM-SM のインタフェース定義が enable であり，QoS 制御などによる中継抑止定義がないことを確認してください。
6. コンフィグレーションで SSM が定義されている場合，G1 が SSM のグループでないことを確認してください。
7. （*,G1）が存在しない場合はランデブーポイント，（S1,G1）が存在しない場合は S1 へのユニキャスト経路が存在することを確認してください。ランデブーポイントは本装置 #2 の装置アドレスです。
8. 本装置 #1 で show ipv6 mroute コマンドを実行し，送信元 S1 から G1 への IPv6 マルチキャストルーティングテーブルが存在していることを確認してください。存在しない場合は，S1 との IPv6 PIM-SM のインタフェース定義が enable であり，QoS 制御などによる抑止定義がないことを確認してください。
9. IPv6 マルチキャストルーティングテーブルの下流が存在しない場合，show ipv6 pim neighbor で本装置 #2 と本装置 #3 が表示されていることを確認してください。また，IPv6 マルチキャストルーティングテーブルが存在しない場合は，show ipv6 pim bsr および show ipv6 pim rendezvous-point mapping

を実行し，BSR およびランデブーポイント（RP）が本装置 #2 であることを確認してください。

10. BSR およびランデブーポイント（RP）が存在しないか本装置 #2 でない場合，本装置 #2 で show ipv6 pim bsr および show ipv6 pim rendezvous-point mapping コマンドを実行し，本装置 #2 が BSR およびランデブーポイント（RP）であることを確認してください。本装置 #2 が BSR およびランデブーポイントでない場合，コンフィグレーションで BSR およびランデブーポイントの定義が正しいか確認してください。
11. 本装置 #2 で show ipv6 mroute コマンドを実行し，送信元 S1 から G1 への IPv6 マルチキャストルーティングテーブル（S1,G1）および G1 への IPv6 マルチキャストルーティングテーブル（*,G1）が存在していることを確認してください。存在しない場合は，本装置 #1 および本装置 #3 との IPv6 PIM-SM のインタフェース定義が enable であり，QoS 制御などによる中継抑止定義がないことを確認してください。
12. IPv6 マルチキャストルーティングテーブルの下流が存在しない場合，show ipv6 pim neighbor で本装置 #1 と本装置 #3 が表示されていることを確認してください。
13. IPv6 マルチキャストルーティングテーブルが存在しない場合は，本装置 #3 で show ipv6 pim bsr および show ipv6 pim rendezvous-point mapping を実行し，BSR およびランデブーポイント（RP）が本装置 #2 であることを確認してください。

（2） PIM-SSM ネットワーク

図に示す IPv6 PIM-SSM ネットワークの構成で，送信元 S1 から G1 宛のパケットがホスト #1 で受信できない場合，次の手順に従って対処してください。

1. すべての本装置で show pru resources コマンドを実行し，PRU 上のハードウェアテーブルに IPv6 マルチキャスト経路を割り当ててあることを確認してください。
2. すべての本装置で QoS 制御などによる中継抑止定義がないことを確認してください。
3. すべての本装置のコンフィグレーションに SSM が定義され，G1 が SSM アドレスであることを確認してください。
4. すべての本装置で show ipv6 pim interface コマンドを実行し，対ルータインタフェースが表示されることを確認してください。表示されない場合はコンフィグレーションを確認してください。また，それぞれのインタフェースがリンクアップしていることを確認してください。
5. すべての本装置で show ipv6 pim interface コマンドを実行し，近隣ルータを認識できていることを確認してください。
6. すべての本装置で S1 へのユニキャスト経路が存在することを確認してください。（ここでは本装置 #4 の上流を本装置 #2 側として説明します）
7. 送信元 S1 のデータ送信を行うインタフェースに S1 が定義されていることを確認してください。複数

個の IPv6 アドレスが設定されている場合（アドレスの自動設定機能が有効になっている場合など）には，送信されるデータの送信元アドレスが S1 であることを確認してください。また，S1 のアドレスが本装置 #1 の直接接続アドレスであることを確認してください。

8. 送信元 S1 が送信するデータが G1 であることを確認してください。違っている場合，本装置 #1 で netstat multicast コマンドを実行するとネガティブキャッシュ (出力インタフェースが存在しないエントリ) が表示されます。
9. 本装置 #4 で show ipv6 mld interface コマンドを実行し，ホスト #1 とのインタフェースが表示されることを確認してください。表示されない場合はコンフィグレーションを確認してください。またそれぞれのインタフェースがリンクアップしていることを確認してください。
10. 対ホストインタフェースの MLD バージョンを確認し，ホストの MLD パケットが受信できる状態であることを確認してください。
11. 本装置 #4 で show ipv6 mld group コマンドを実行し，G1 グループにホスト #1 が参加していることを確認してください。
12. ホストが MLDv1 の場合，本装置 #4 で ssm-join のコンフィグレーションに（G1,S1）に該当する定義が存在することを確認してください。また，show ipv6 mld group コマンドを実行し，参加した G1 グループに対する送信元情報 S1 が登録されていることを確認してください。
13. ホストが MLDv2 の場合，show ipv6 mld group コマンドを実行し，参加した G1 グループに対する送信元情報 S1 が登録されていることを確認してください。
14. 本装置 #4 で show ipv6 mroute コマンドを実行し，送信元 S1 から G1 への IPv6 マルチキャストルーティングテーブル（S1,G1）が存在していることを確認してください。存在する場合は，iif が #2 側のインタフェースで，oif がホスト #1 側のインタフェースの SSM エントリであることを確認してください。存在しない場合は，本装置と #2 の IPv6 PIM-SM のインタフェース定義が enable であることを確認してください。
15. 本装置 #2 で show ipv6 mroute コマンドを実行し，送信元 S1 から G1 への IPv6 マルチキャストルーティングテーブル（S1,G1）が存在していることを確認してください。存在する場合は，iif が装置 #1 側のインタフェースで，oif が装置 #4 側のインタフェースである SSM エントリであることを確認してください。存在しない場合は，本装置 #4 および本装置 #1 との PIM-SM のインタフェース定義が enable であることを確認してください。
16. 本装置 #1 で show ipv6 mroute コマンドを実行し，送信元 S1 から G1 への IPv6 マルチキャストルーティングテーブル（S1,G1）が存在していることを確認してください。存在する場合は，iif が S1 のインタフェースで，oif が装置 #2 側のインタフェースの SSM エントリであることを確認してください。

8.11 MPLS の通信障害【OP-MPLS】

MPLS 関連で通信トラブルが発生した場合は，以下に従って障害を取り除いてください。

8.11.1 MPLS 通信障害の切り分け

(1) 注意事項の確認

通信障害の切り分けを開始する前に，発生している現象が「解説書 Vol.1　16. MPLS【OP-MPLS】」に書かれている注意事項に該当しないか確認してください。注意事項に該当しない場合，「(2) MPLS 通信障害の切り分け」から障害解析を開始してください。

(2) MPLS 通信障害の切り分け

本装置の MPLS 通信では，大きく分けて次の三つの通信種別をサポートしています。通信種別によって切り分け手順が異なります。次の表に従って，適切な障害切り分け手順を参照してください。

表 8-30　通信種別ごとの障害切り分け手順

項番	通信種別	切り分け手順
1	非 VPN MPLS 通信の障害	詳細な障害切り分け手順は，「8.11.2　非 VPN MPLS 通信の障害」を参照してください。
2	IP-VPN のサイト間通信の障害	詳細な障害切り分け手順は，「8.11.3　IP-VPN のサイト間通信の障害」を参照してください。
3	EoMPLS(L2-VPN) のサイト間通信の障害	詳細な障害切り分け手順は，「8.11.4　EoMPLS(L2-VPN) のサイト間通信の障害」を参照してください。

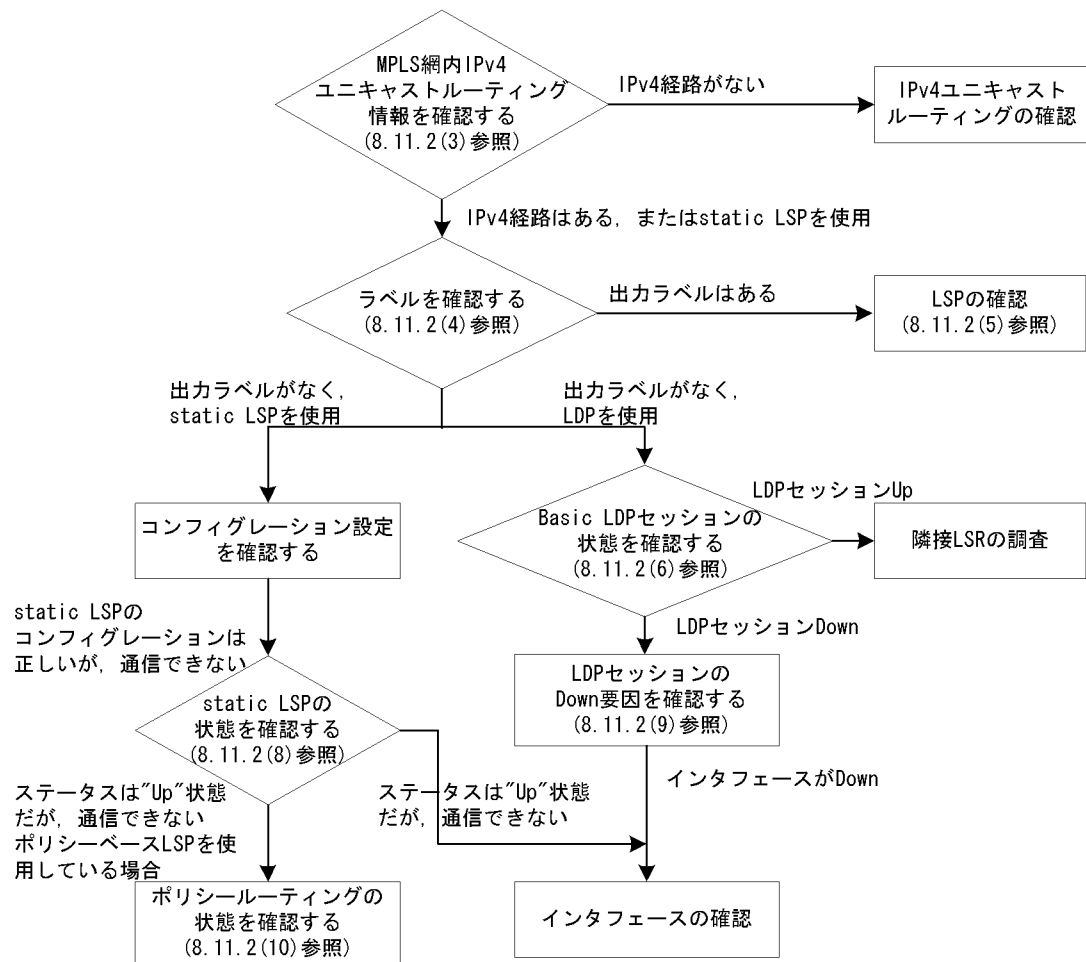
8.11.2 非 VPN MPLS 通信の障害

(1) MPLS 網内の障害個所 (装置) の切り分け

MPLS 網を構成している複数の LSR の中から，障害が発生している LSR を切り分けます。ping mpls, traceroute mpls コマンドを使ってエッジ LSR からの疎通を確認します。一方向の LSP の疎通だけでなく，両方向の LSP について両端のエッジ LSR から疎通を確認してください。詳細な確認方法については，「6.1.1　イーサネット回線の動作状態を確認する」を参照してください。

(2) 非 VPN MPLS 通信の障害切り分け手順

非 VPN MPLS 通信において障害が発生した場合，次の手順に従って，障害切り分けを行ってください。

図 8-9 非 VPN MPLS 通信の障害切り分け手順

(3) MPLS 網内 IPv4 ユニキャストルーティング情報を確認する

「6.9.1 非 VPN MPLS 通信を確認する (3) MPLS 網内 IPv4 ユニキャストルーティング情報の確認」に従って，通信できないサイト間の MPLS 網内の IPv4 ユニキャストルーティング情報を確認してください。

- IPv4 ユニキャストルーティング情報がある，または static LSP を使っている場合
  「(4) ラベルを確認する」に進んでください。
- IPv4 ユニキャストルーティング情報がない場合
  「8.6 IPv4 ユニキャストルーティングの通信障害」に進んでください。

(4) ラベルを確認する

「6.9.1 非 VPN MPLS 通信を確認する (4) MPLS ラベルを確認する」に従って，リモートサイトに対する出力ラベルを確認してください。

- 出力ラベルがある場合
  「(5) LSP の確認」に進んでください。
- 出力ラベルがない場合
  - LDP を使って LSP を設定している場合
    「(6) Basic LDP セッションの状態を確認する」に進んでください。

- Static LSP を使って LSP を設定している場合
「（7）static LSP コンフィグレーションを確認する」に進んでください。

（5）LSP の確認

traceroute コマンド（mpls オプションなし）で，MPLS 網内のルートを表示します。最後に応答したルータまたはその次のルータで障害が発生している可能性があります。該当するルータを確認してください。

［注意事項］

- ダイレクト経路への送信
VPN でない IP パケットを送信するとき，宛先 IP アドレスへの IPv4 ユニキャストルーティング情報が，本装置のダイレクト経路または隣接 LSR のダイレクト経路であった場合，MPLS パケットとしてではなく，通常の IP パケットとして送信します。例えば本装置から，Core ルータを 1 台だけ経由する出口エッジルータに ping コマンド（mpls オプションなし）や traceroute コマンド（mpls オプションなし）を実行する際，出口エッジルータの Core ルータとのインタフェースの IP アドレスを指定すると，本装置が送信するパケットは MPLS パケットとなりません。
- 非 VPN 通信の出口エッジルータでの受信
非 VPN 通信では，PHP により出口エッジルータ直前の LSR からはラベルが省略され，通常の IPv4 パケットになります。
- 網内マルチパス経路での非 VPN 通信
網内経路がマルチパス経路の場合，そのマルチパス内の一つの経路を選択しての MPLS 通信となります。
- traceroute コマンド（mpls オプションなし）のラベル表示
本装置で MPLS 通信する LSR またはリモートサイトに対して traceroute コマンド（mpls オプションなし）を実行すると，応答するルータが応答にラベル値を埋め込んだ場合にそのラベル値が表示されます。応答するルータによっては，応答にラベル値を埋め込まないため，MPLS 通信をしていても traceroute コマンド（mpls オプションなし）でラベル値が表示されないことがあります。

（6）Basic LDP セッションの状態を確認する

MPLS 通信には，IPv4 ユニキャストルーティング情報の出力インタフェースで Basic LDP セッションの状態が UP となっている必要があります。「6.9.1　非 VPN MPLS 通信を確認する　（5）Basic LDP セッションの状態を確認する」に従って，Basic LDP セッションの状態を確認します。

- 状態が UP 以外の場合
Basic LDP を使って LSP を設定している場合，「（9）LDP セッションの DOWN 要因を確認する」に進んでください。
- 状態が UP の場合
隣接する LSR からラベルが配布されていません。隣接 LSR を調査してください。

（7）static LSP コンフィグレーションを確認する

static LSP を使って LSP を設定している場合，コンフィグレーションを確認してください。コンフィグモードに入り，show mpls static-lsp コマンドで確認できます。

static LSP コンフィグレーションは正しいが通信ができない場合は，「（8）static LSP の状態を確認する」へ進んでください。

（8）static LSP の状態を確認する

static LSP を使って LSP を設定している場合，show mpls static-lsp status コマンドによって，static

LSP のステータス情報を確認します。「6.9.1　非 VPN MPLS 通信を確認する　(7) static LSP の状態を確認する」に従って，static LSP のステータス状態を確認してください。

- staticLSP の状態が UP だが policy-base の static LSP を使っている場合
  policy-base の static LSP を使っている場合で，static LSP のステータスが UP 状態にも関わらず通信ができないときは，ポリシールーティングの状態を確認する必要があります。「(10) ポリシールーティングの状態を確認する」へ進んでください。
- static LSP の状態が Down の場合
  インタフェースの状態を確認してください。

(9) LDP セッションの DOWN 要因を確認する

LDP セッションで指定した IP アドレスのインタフェースの状態を確認してください。

- インタフェースの状態が UP でない場合
  「8.4　ネットワークインタフェースの通信障害」に従って，インタフェースの障害を取り除いてください。
- インタフェースの状態が UP になっている場合
  インタフェースの状態が UP になっているにも関わらず，LDP セッションが DOWN している場合は，show mpls ldp コマンドで detail オプションを指定し，Basic LDP セッションが確立しない原因を調査してください。詳細な確認方法については「6.9.1　非 VPN MPLS 通信を確認する　(6) Basic LDP セッションダウンの要因を確認する」を参照してください。

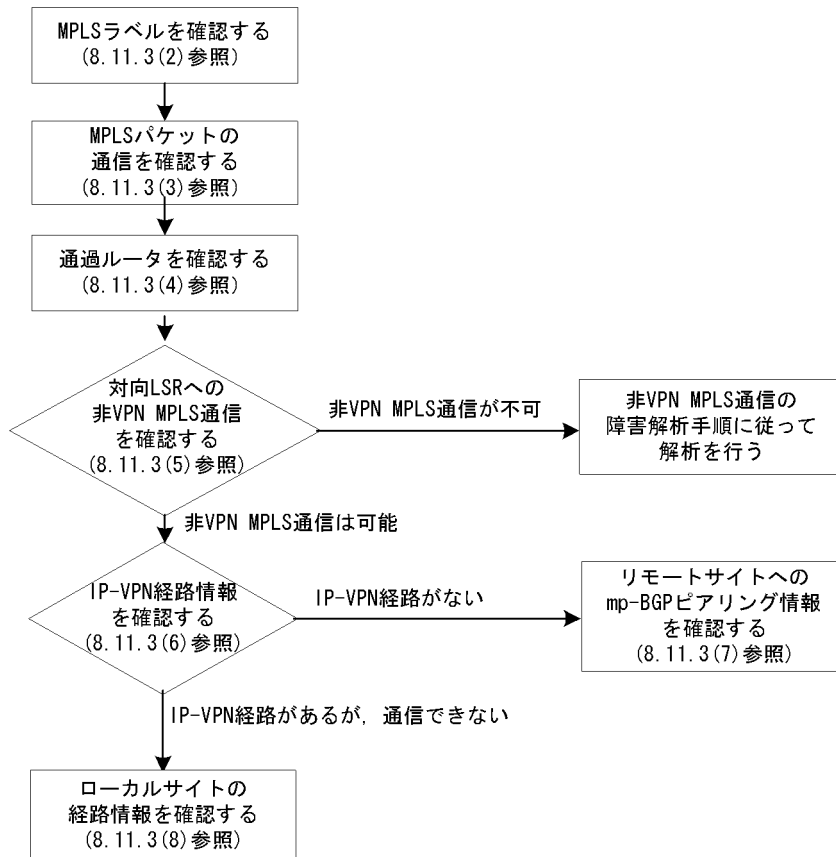
(10) ポリシールーティングの状態を確認する

policy-base の static LSP を使用している場合，対象とする通信フレームに正しくポリシールーティングが適用されているかを確認してください。show filter-flow コマンドによって該当するポリシールーティング条件にヒットしていることを確認してください。詳細な確認方法については，「6.9.1　非 VPN MPLS 通信を確認する　(8) ポリシールーティングの状態を確認する」を参照してください。

8.11.3　IP-VPN のサイト間通信の障害

(1) IP-VPN のサイト間通信の障害切り分け手順

IP-VPN サイト間通信において障害が発生した場合，次の手順に従って，障害切り分けを行ってください。

図 8-10　IP-VPN 通信の障害切り分け手順

(2) MPLS ラベルを確認する

「6.9.2　IP-VPN 通信を確認する　(4) MPLS ラベルを確認する」に従って，リモートサイトに対する出力ラベルとローカルサイトに対する入力ラベルを確認します。

(3) MPLS パケットの通信を確認する

「6.9.2　IP-VPN 通信を確認する　(5) MPLS パケットの通信を確認する」に従って，MPLS パケットの到達性を確認できます。

(4) 通過ルータを確認する

「6.9.2　IP-VPN 通信を確認する　(6) 通過ルータを確認する」に従って，宛先アドレスまでの通過ルータを確認できます。

(5) 対向 LSR への非 VPN MPLS 通信を確認する

IP-VPN 通信では，対向 LSR のローカルアドレス (BGP ピアの IP アドレス) への非 VPN MPLS 通信が可能である必要があります。「6.9.2　IP-VPN 通信を確認する　(1) 対向 LSR への非 VPN MPLS 通信の確認」に従って，対向 LSR のローカルアドレスに対する出力ラベルを中心に，非 VPN MPLS 通信を確認してください。

- 非 VPN MPLS 通信は可能である場合
  「(6) IP-VPN 経路情報を確認する」に進んでください。
- 非 VPN MPLS 通信が不可の場合

「8.11.2　非 VPN MPLS 通信の障害」に従って，MPLS 網通信の確認を行ってください。

(6)　IP-VPN 経路情報を確認する

「6.9.2　IP-VPN 通信を確認する　(2) IP-VPN 経路情報を確認する」に従って IP-VPN 経路情報を確認します。本装置が取得した経路情報を確認してください。

- IP-VPN 経路情報がある場合
  「(8)　ローカルサイトの経路情報を確認する」を参照してください。
- IP-VPN 経路情報がない場合
  「(7)　リモートサイトへの mp-BGP ピアリング情報を確認する」に進んでください。

(7)　リモートサイトへの mp-BGP ピアリング情報を確認する

「6.9.2　IP-VPN 通信を確認する　(3) mp-BGP のピアリング情報を確認する」に従って mp-BGP ピアリングの状態を確認します。

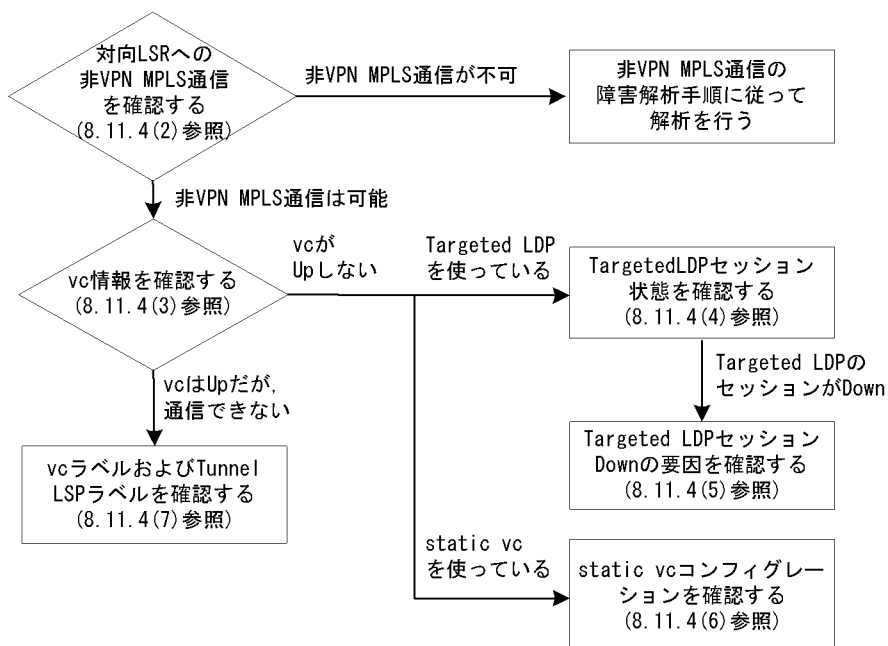
(8)　ローカルサイトの経路情報を確認する

「8.6.1　RIP 経路情報がない」〜「8.6.3　BGP4 経路情報がない【OP-BGP】」を参照してローカルサイトのルーティングプロトコル情報を確認してください。確認する場合にはコマンドパラメータに vpn を指定してください。

8.11.4　EoMPLS(L2-VPN) のサイト間通信の障害

(1)　EoMPLS(L2-VPN) のサイト間通信の障害切り分け手順

EoMPLS(L2-VPN) のサイト間通信において障害が発生した場合，次の手順に従って，障害切り分けを行ってください。

図 8-11　EoMPLS(L2-VPN) 通信の障害切り分け手順

（2） 対向 LSR への非 VPN MPLS 通信の確認

EoMPLS(L2-VPN) 通信では，対向 LSR のローカルアドレス (BGP ピアの IP アドレス) への非 VPN MPLS 通信が可能である必要があります。「6.9.3　EoMPLS(L2-VPN) 通信を確認する　(1) 対向 LSR への非 VPN MPLS 通信の確認」に従って，対向 LSR のローカルアドレスに対する出力ラベルを中心に，非 VPN MPLS 通信を確認してください。

- 非 VPN MPLS 通信は可能である場合
  「(3) VC 情報を確認する」に進んでください。
- 非 VPN MPLS 通信が不可の場合
  「8.11.2　非 VPN MPLS 通信の障害」に従って，MPLS 網通信の確認を行ってください。

（3） VC 情報を確認する

「6.9.3　EoMPLS(L2-VPN) 通信を確認する　(2) EoMPLS(L2-VPN) の VC の状態を確認する」に従って，通信できないサイト間の VC の状態を確認してください。

- VC の状態が UP の場合
  「(7) VC ラベル，および Tunnel LSP ラベルを確認する」に進んでください。
- VC の状態が UP 以外の場合
  - Targeted LDP を使って VC を設定している場合
    「(4) Targeted LDP セッション状態を確認する」へ進んでください。
  - static vc を使って VC を設定している場合
    「(6) static vc コンフィグレーションを確認する」へ進んでください。

（4） Targeted LDP セッション状態を確認する

「6.9.3　EoMPLS(L2-VPN) 通信を確認する　(3) Targeted LDP セッション状態を確認する」に従って，Targeted LDP のセッション Up/Down を確認してください。セッションが Down しているならば，「(5) Targeted LDP セッション Down の要因を確認する」へ進んでください。

（5） Targeted LDP セッション Down の要因を確認する

「6.9.3　EoMPLS(L2-VPN) 通信を確認する　(4) Targeted LDP セッション Down の要因を確認する」に従って，Targeted LDP セッションが Down する原因を確認してください。

（6） static vc コンフィグレーションを確認する

static vc コンフィグレーションを確認してください。コンフィグモードに入り，show mpls l2transport コマンドで確認できます。

（7） VC ラベル，および Tunnel LSP ラベルを確認する

「6.9.3　EoMPLS(L2-VPN) 通信を確認する　(5) VC ラベル，および Tunnel LSP ラベルを確認する」に従って，EoMPLS(L2-VPN) に関わるラベル情報を確認してください。

8.12　高信頼性機能の通信障害

8.12.1　IPv4 ネットワークの VRRP 構成で通信ができない

VRRP 構成で通信ができない場合は，次の表に示す障害解析方法に従って原因の切り分けおよび情報収集を行ってください。

表 8-31　VRRP の障害解析方法

項番	確認内容・コマンド	対応
1	同一仮想ルータを構成する相手装置と本装置において仮想ルータの状態を確認し，マスタルータとなっている装置が 1 台でありほかの装置はバックアップになっていることを確認してください。	同一仮想ルータを構成する装置間で，マスタ状態となっている装置が 1 台だけであり，そのほかはバックアップとなっている場合には，本装置を含めた通信経路上の装置での経路情報を確認してください。
		仮想ルータの状態が正しい場合は項番 2 へ。
2	同一仮想ルータを構成する相手装置と本装置の仮想ルータの状態が，お互いにマスタ状態となっていないことを確認してください。	複数の仮想ルータがマスタ状態となっている場合は項番 3 へ。
		複数の仮想ルータがマスタ状態となっていない場合は項番 5 へ。
3	ping コマンドで，マスタルータ間の通信を実 IPv4 アドレスで確認してください。	マスタルータ間の実 IPv4 アドレスによる通信ができない場合，仮想ルータを構成するルータ間の物理的なネットワーク構成を確認してください。
		マスタルータ間の実 IPv4 アドレスを用いた ping コマンドによる確認ができた場合は項番 4 へ。
4	show vrrpstatus detail コマンドにより VRRP の統計情報を確認してください。	VRRP の受信パケットにエラーが発生している場合は，本装置と相手装置のコンフィグレーションを再確認してください。
		VRRP のパケットが正常に受信されている場合は，相手装置を確認してください。受信されていない場合には，ネットワークの物理構成を確認してください。
5	障害監視インタフェース定義がある場合，障害監視インタフェースの状態を確認してください。	障害監視インタフェースを定義したインタフェースに別の仮想ルータの定義があり，その仮想ルータの障害監視インタフェースが該当仮想ルータのインタフェースになっていないことを確認してください。なっている場合は，どちらかの障害インタフェースの定義を削除してください。
		上記の障害監視インタフェースの定義がない場合は項番 6 へ。
6	フィルタの定義で VRRP の Advertisement パケットを廃棄する設定がないことを確認してください。	該当するフィルタの定義がある場合，VRRP の Advertisement を廃棄しないようにフィルタの定義を変更してください。
		フィルタの定義がない場合，同一の仮想ルータを構成する相手装置の動作を確認してください。

項番	確認内容・コマンド	対応
7	仮想 MAC アドレス宛の中継ができない。	show tech-support コマンド（詳細は「9.1　障害情報の取得」を参照してください）に加え，以下の VRRP の情報収集を行ってください。 • show vrrpstatus detail（画面ログ） • show vrrpstatus statistics（画面ログ） • cat　/var/log/daemon.log (画面ログ) • /usr/local/bin/vrrpstat -Z ※ → /primaryMC/usr/var/vrrp/vrrpdump ファイルの収集 • /usr/local/bin/vrrpstat -X (画面ログ) ※ • /usr/local/bin/vrrpstat -X sendcmd dump,portmap ※ → /primaryMC/usr/var/vrrp/vrrpportmap ファイルの収集 • /usr/local/bin/vrrpstat -X sendcmd dump,l2talk ※ → /primaryMC/usr/var/vrrp/l2talkdump ファイルの収集

注※　補完がありません。

8.12.2　IPv6 ネットワークの VRRP 構成で通信ができない

VRRP 構成で通信ができない場合は，次の表に示す障害解析方法に従って原因の切り分けおよび情報収集を行ってください。

表 8-32　VRRP の障害解析方法

項番	確認内容・コマンド	対応
1	同一仮想ルータを構成する相手装置と本装置において仮想ルータの状態を確認し，マスタルータとなっている装置が 1 台でありほかの装置はバックアップになっていることを確認してください。	同一仮想ルータを構成する装置間で，マスタ状態となっている装置が 1 台だけであり，そのほかはバックアップとなっている場合には，本装置を含めた通信経路上の装置での経路情報を確認してください。
		仮想ルータの状態が正しい場合は項番 2 へ。
2	同一仮想ルータを構成する相手装置と本装置の仮想ルータの状態が，お互いにマスタ状態となっていないことを確認してください。	複数の仮想ルータがマスタ状態となっている場合は項番 3 へ。
		複数の仮想ルータがマスタ状態となっていない場合は項番 5 へ。
3	ping ipv6 コマンドで，マスタルータ間の通信を実 IPv6 アドレスで確認してください。	マスタルータ間の実 IPv6 アドレスによる通信ができない場合，仮想ルータを構成するルータ間の物理的なネットワーク構成を確認してください。
		マスタルータ間の実 IPv6 アドレスを用いた ping ipv6 コマンドによる確認ができた場合は項番 4 へ。
4	show vrrpstatus detail コマンドにより VRRP の統計情報を確認してください。	VRRP の受信パケットにエラーが発生している場合は，本装置と相手装置のコンフィグレーションを再確認してください。
		VRRP のパケットが正常に受信されている場合は，相手装置を確認してください。受信されていない場合には，ネットワークの物理構成を確認してください。
5	障害監視インタフェース定義がある場合，障害監視インタフェースの状態を確認してください。	障害監視インタフェースを定義したインタフェースに別の仮想ルータの定義があり，その仮想ルータの障害監視インタフェースが該当仮想ルータのインタフェースになっていないことを確認してください。なっている場合は，どちらかの障害インタフェースの定義を削除してください。
		上記の障害監視インタフェースの定義がない場合は項番 6 へ。

項番	確認内容・コマンド	対応
6	フィルタの定義で VRRP の Advertisement パケットを廃棄する設定がないことを確認してください。	該当するフィルタの定義がある場合，VRRP の Advertisement を廃棄しないようにフィルタの定義を変更してください。
		フィルタの定義がない場合，同一の仮想ルータを構成する相手装置の動作を確認してください。
7	仮想 MAC アドレス宛の中継ができない。	show tech-support コマンド（詳細は「9.1　障害情報の取得」を参照してください）に加え，以下の VRRP の情報収集を行ってください。 • show vrrpstatus detail（画面ログ） • show vrrpstatus statistics（画面ログ） • cat /var/log/daemon.log (画面ログ) • /usr/local/bin/vrrpstat -Z ※ → /primaryMC/usr/var/vrrp/vrrpdump ファイルの収集 • /usr/local/bin/vrrpstat -X (画面ログ) ※ • /usr/local/bin/vrrpstat -X sendcmd dump,portmap ※ → /primaryMC/usr/var/vrrp/vrrpportmap ファイルの収集 • /usr/local/bin/vrrpstat -X sendcmd dump,l2talk ※ → /primaryMC/usr/var/vrrp/l2talkdump ファイルの収集

注※　補完がありません。

8.12.3　IEEE802.3ah/UDLD 機能でポートが閉塞状態になる

IEEE802.3ah/UDLD 機能によってポートが閉塞される場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 8-33　IEEE802.3ah/UDLD 機能使用時の障害解析方法

項番	確認内容・コマンド	対応
1	show efmoam コマンドを実行し，IEEE802.3ah/UDLD 機能で閉塞状態にしたポートの障害種別を確認してください。	Link status が Down(loop) と表示されている場合は，ネットワーク構成が L2 ループになっている可能性があります。ネットワーク構成を見直してください。
		Link status が Down(uni-link) と表示されている場合は，項番 2 へ。
2	対向装置で IEEE802.3ah/OAM 機能が有効であることを確認してください。	対向装置側で IEEE802.3ah/OAM 機能が有効となっていない場合は有効になるよう設定してください。
		対向装置側で IEEE802.3ah/OAM 機能が有効になっている場合は項番 3 へ。
3	show efmoam statistics コマンドを実行し，禁止構成になっていないことを確認してください。	Info TLV の Unstable がカウントアップされている場合は，IEEE802.3ah/UDLD 機能の禁止構成になっている可能性があります。該当物理ポートの接続先装置が 1 台であることを確認してください。
		Info TLV の Unstable がカウントアップされていない場合は項番 4 へ。
4	対向装置と直接接続されていることを確認してください。	メディアコンバータやハブ等が介在している場合は，直接接続できるようにネットワーク構成を見直してください。どうしても直接接続できない場合は，両側のリンク状態が連動するメディアコンバータを使用してください（ただし推奨はしません）。
		直接接続されている場合は項番 5 へ。
5	show efmoam コマンドを実行し，障害を検出するための応答タイムアウト回数を確認してください。	udld-detection-count が初期値未満の場合，実際に障害となっていない場合でも片方向リンク障害を誤検出する可能性があります。この値を変更してください。

項番	確認内容・コマンド	対応
		udld-detection-count が初期値以上の場合は項番 6 へ。
6	回線のテストを行ってください。	「9.7　回線をテストする」を参照し，回線のテストを行ってください。 問題がない場合は項番 7 へ。
7	ケーブルを確認してください。	ケーブル不良の可能性があります。該当ポートで使用しているケーブルを交換してください。

注　IEEE802.3ah/OAM：IEEE802.3ah で規定されている OAM プロトコル

IEEE802.3ah/UDLD：IEEE802.3ah/OAM を使用した本装置特有の片方向リンク障害検出機能

8.13　SNMP の通信障害

8.13.1　SNMP マネージャから MIB の取得ができない

次に示す手順で確認してください。

1. コンフィグレーションが正しく登録されていることを確認してください。

SNMPv1，または SNMPv2c を使用する場合

コンフィグレーションコマンド show snmp を実行し，本装置のコンフィグレーションに SNMP マネージャに関する情報が登録されているかどうかを確認してください。
登録されていない場合は，コンフィグレーションコマンド snmp を実行して，SNMP マネージャに関する情報を定義してください。

```
(config)# show snmp
snmp  "public" 20.1.1.1 read_write none
snmp  "public" 10.1.1.1 read ex_trap level 7
```

SNMPv3 を使用する場合

以下のコンフィグレーションコマンドを実行し，本装置のコンフィグレーションに SNMP に関する情報が正しく登録されているかどうかを確認してください。正しく登録されていない場合は，コンフィグレーションコマンドを実行して，SNMP に関する情報を定義してください。

- show snmpv3
- show snmp-engineid
- show snmp-view
- show snmp-user
- show snmp-group

2. コンフィグレーションは正しく登録されているが，SNMP マネージャからの要求に対して応答タイムアウトする場合，SNMP マネージャ側の応答タイムアウト値を少なくとも 5 秒以上に設定してください。
   なお，ネットワークのレスポンスが悪い（SNMP マネージャと本装置間の回線速度が低い，SNMP マネージャと本装置の間に多数の接続装置（ブリッジ，ルータ，スイッチなど）がある）場合は，応答タイム値をさらに延ばす必要があります。
3. SNMP マネージャ側の応答タイムアウト値を変更しても，MIB の取得ができない場合，SNMP マネージャと本装置との間で SNMP フレームのフィルタリング（廃棄）がされている可能性があります。
   ネットワーク管理者に SNMP フレームのフィルタリングがされていないか確認してください（SNMP フレームは，ポート番号 161 の UDP フレームを使って通信しています）。

8.13.2　SNMP マネージャでトラップが受信できない

次に示す手順で確認してください。

1. コンフィグレーションが正しく登録されていることを確認してください。

   SNMPv1，または SNMPv2c を使用する場合

   コンフィグレーションコマンド show snmp を実行し，本装置のコンフィグレーションに SNMP マネージャおよびトラップに関する情報が登録されているかどうかを確認してください。
   登録されていない場合は，コンフィグレーションコマンド snmp を実行して，SNMP マネージャおよびトラップに関する情報を定義してください。

```
(config)# show snmp
snmp "public" 20.1.1.1 read_write none
snmp "public" 10.1.1.1 read ex_trap level 7
snmp "event-monitor" 30.1.1.1 read trap
!
(config)#
```

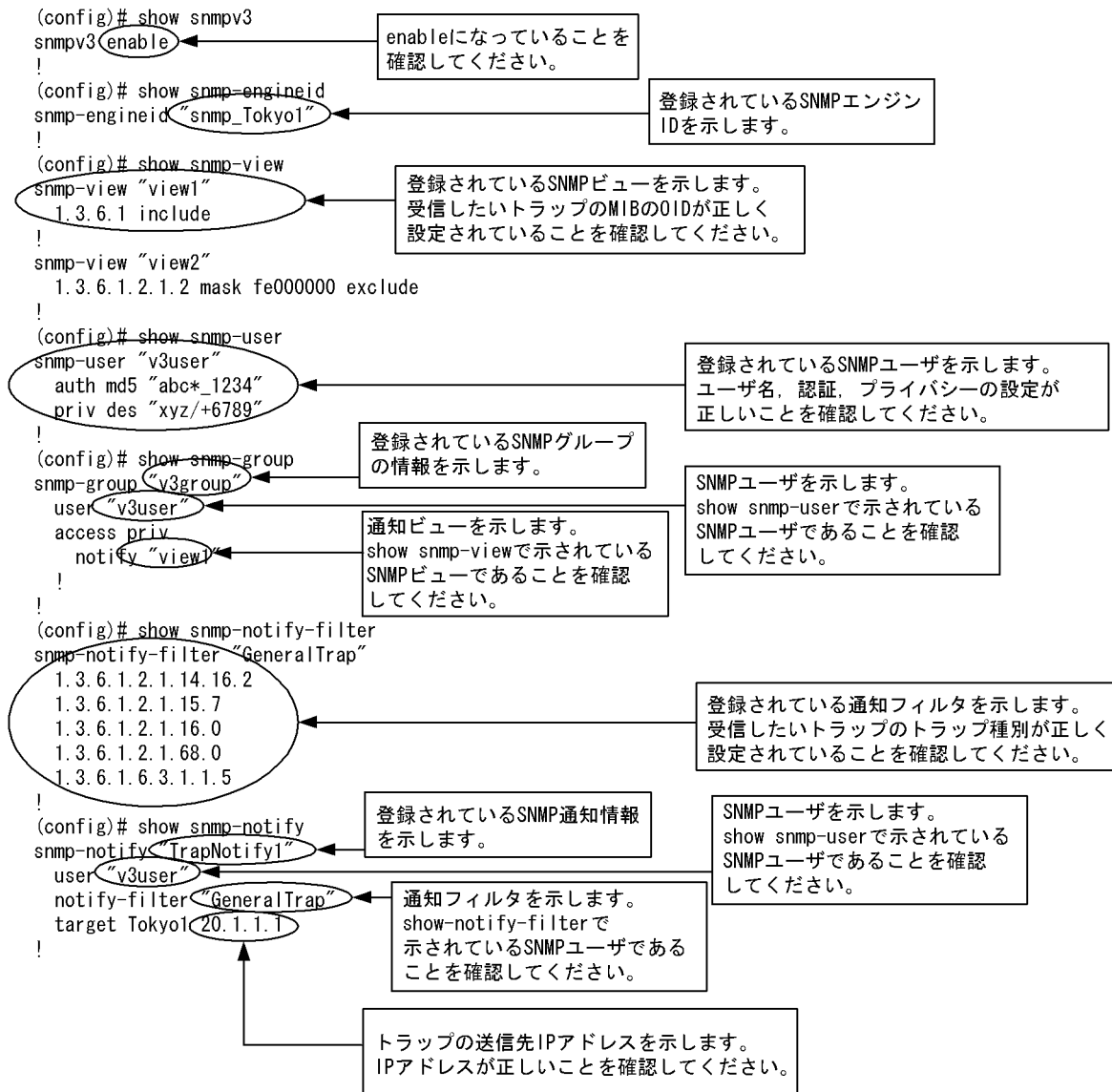
登録されているSNMPマネージャのコミュニティ名称を示します

trapまたはex-trapの表示がされていることを確認してください

登録されているSNMPマネージャのIPアドレスを示します

SNMPv3 を使用する場合

以下のコンフィグレーションコマンドを実行し，本装置のコンフィグレーションにSNMPに関する情報およびトラップに関する情報が正しく登録されているかどうかを確認してください。正しく登録されていない場合は，コンフィグレーションコマンドを実行して，SNMPに関する情報およびトラップに関する情報を定義してください。

- show snmpv3
- show snmp-engineid
- show snmp-view
- show snmp-user
- show snmp-group
- show snmp-notify-filter
- show snmp-notify

2. コンフィグレーションは正しく定義されているがトラップを受信しない場合，SNMP マネージャと本装置との間で SNMP フレームのフィルタリング（廃棄）がされている可能性があります。ネットワーク管理者に SNMP フレームのフィルタリングがされていないか確認してください（SNMP のトラップは，ポート番号 162 の UDP フレームを使って通信しています）。

8.14　フロー統計機能の通信障害

8.14.1　コレクタ装置に sFlow パケットが届かない (sFlow 統計)

（1） コンフィグレーションの確認

以下の観点で，運用中のコンフィグレーションを確認してください。

- sFlow 統計の「フロー統計スイッチ」が”no”であると，ほかのインタフェース情報が正しく設定されていても sFlow 統計は取らないので注意してください。

図 8-12　コンフィグレーション表示例 1

```
(config)# show sflow
sflow yes                 ◄────────  ここがyesになっていること
    destination 192.1.1.1
    sample 128
    port 1/1
!
(config)#
```

- コンフィグレーションの中に sFlow パケットの送信先であるコレクタ装置の IP アドレスと UDP ポート番号が正しく設定されていることを確認してください。

図 8-13　コンフィグレーション表示例 2

```
(config)# show sflow
sflow yes
    destination 192.1.1.1 udp 6455 ◄────  コレクタ情報が正しく設定されていること
    sample 128
    port 1/1
!
(config)#
```

- サンプリング間隔の設定がされていることを確認してください。サンプリング間隔が設定されていないとデフォルト値 (536870912) の大きな値で動作するため，フローサンプルがコレクタ装置にほとんど送信されません。適切なサンプリング間隔を設定してください。推奨値より極端に小さな値を設定した場合，ソフトウェア処理性能に影響がでてくる可能性があります。

図 8-14　コンフィグレーション表示例 3

```
(config)# show sflow
sflow yes
    destination 192.1.1.1
    sample 32
    port 1/1
         port-sample 512
    port 3/1
         port-sample 2048
!
(config)#
```

利用環境に応じた適切なサンプリング間隔が設定されていること

● 同一の PRU 内で大きな値のサンプリング間隔が設定されていないことを確認してください。PRU 内で一番大きな値を PRU 内すべてのポートのサンプリング間隔として使用するため，一部のサンプリング間隔が大きいとフローサンプルがコレクタ装置に期待どおりに送信されません。

図 8-15　コンフィグレーション表示例 4

```
(config)# show sflow
sflow yes
    destination 192.1.1.1
    sample 32
    port 0/1
         port-sample 512
    port 1/1
         port-sample 2048
    port 1/2
         port-sample 524288
!
(config)#
```

実際はPRU内で一番大きなサンプリング間隔(524288)で動作します

図 8-16　運用コマンド情報表示例 1

```
> show sflow detail
sFlow service status: enable
       ～中略～
Configured sFlow port: 0/1 , 1/1 - 1/2
Sampling port rates:
Port:0/1  Configured rate:512  Actual rate:524288

Port:1/1  Configured rate:2048  Actual rate:524288
Port:1/2  Configured rate:524288  Actual rate:524288
```

Actual rateが大きな値になっていませんか？

● フロー統計を行いたい物理ポートに対し forward-off 設定が行われていないことを確認してください。

図 8-17　コンフィグレーション表示例 5

```
(config)# show sflow
sflow yes
    destination 192.1.1.1
    sample 128
    port 1/1  ◀──────── ここにforward-off設定がされていないこと
!
(config)#
```

(2) インタフェース情報の確認

sFlow 統計で使用する本装置のインタフェース状態を，show interface コマンドを実行することにより，監視する物理ポートの up/down 状態が”active up”（正常動作中）であることを確認してください。

図 8-18　インタフェース状態表示例

```
> show interface nif 0 line 0
2003/04/02 12:00:00
NIF0: active 1-port 1000BASE-SX retry:2
           Average:700/2000Mbps Peak:750Mbps at 10:10:12
Line0:active up 1000BASE-SX full 00:12:E2:45:0a:01
           Protocol:up
           IP address:10.0.0.2 Broadcast IP address:10.0.0.255
(以下省略)
>
```

インタフェースが DOWN 状態の場合は，「8.5.1　通信ができない，または切断されている」を参照してください。

(3) コレクタ装置との通信の確認

sFlow 統計で使用するコレクタ装置との通信が確立されているか，コマンドラインから ping コマンドを実行することにより確認してください。

図 8-19　コレクタ装置との通信確立確認例

```
> ping 192.1.1.1
pinging 192.1.1.1 with 32 bytes of data:

reply from 192.1.1.1: bytes=32 time<10ms TTL=128
reply from 192.1.1.1: bytes=32 time<10ms TTL=128
reply from 192.1.1.1: bytes=32 time<10ms TTL=128
reply from 192.1.1.1: bytes=32 time<10ms TTL=128

Ping statistics for 192.1.1.1:
    Packet: Sent = 4, Received = 4,Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
>
```

8.14.2　フローサンプルがコレクタに届かない (sFlow 統計)

次に示す手順で確認してください。

- サンプリング間隔の設定がされていることを確認してください。サンプリング間隔が設定されていないとデフォルト値 (536870912) の大きな値で動作するため，フローサンプルがコレクタ装置にほとんど送信されません。

図 8-20　コンフィグレーション表示例 6

```
(config)# show sflow
sflow yes
    destination 192.1.1.1
    sample 32
    port 1/1
         port-sample 512
    port 3/1
         port-sample 2048
!
(config)#
```

利用環境に応じた適切なサンプリング間隔が設定されていること

● 同一の PRU 内で大きな値のサンプリング間隔が設定されていないことを確認してください。PRU 内で一番大きな値を PRU 内すべてのポートのサンプリング間隔として使用するため，一部のサンプリング間隔が大きいとフローサンプルがコレクタ装置にほとんど送信されません。

図 8-21　コンフィグレーション表示例 7

```
(config)# show sflow
sflow yes
    destination 192.1.1.1
    sample 32
    port 0/1
         port-sample 512
    port 1/1
         port-sample 2048
    port 1/2
         port-sample 524288
!
(config)#
```

実際はPRU内で一番大きなサンプリング間隔(524288)で動作します

図 8-22　運用コマンド情報表示例 2

```
> show sflow detail
sFlow service status: enable
       ～中略～
Configured sFlow port: 0/1 , 1/1 - 1/2
Sampling port rates:
Port:0/1  Configured rate:512  Actual rate:524288

Port:1/1  Configured rate:2048  Actual rate:524288
Port:1/2  Configured rate:524288  Actual rate:524288
```

Actual rateが大きな値になっていませんか？

8.14.3　カウンタサンプルがコレクタに届かない (sFlow 統計)

本装置のコンフィグレーションにフロー統計に関するカウンタサンプルの通知間隔の情報が 0 になってい

ないかを確認してください。この値が 0 になっているとカウンタサンプルのデータがコレクタへ送信されません。

図 8-23　コンフィグレーション表示例 8

```
(config)# show sflow
sflow yes
    destination 192.1.1.1
    polling-interval 60    ◀────  ここに0が設定されていないこと
    sample 128
    port 1/1
!
(config)#
```

8.14.4　コレクタ装置に NetFlow パケットが届かない (NetFlow 統計)

(1)　コンフィグレーションの確認

以下の観点で，運用中のコンフィグレーションを確認してください

● NetFlow 統計の「フロー統計スイッチ」が”no”であると，ほかのインタフェース情報が正しく設定されていても NetFlow 統計は取らないので注意してください。

図 8-24　コンフィグレーション表示例 9

```
(config)# show netflow
netflow yes   ← ここが yes になっていること
    sample 2048
    entries 0 4000
    flow-export-version 5
            destination 172.16.178.2 udp 1234
    port 1/1-2
!
(config)#
```

● サンプリング間隔の設定がされていることを確認してください。サンプリング間隔が設定されていないと動作しません。必ず設定してください。

図 8-25　コンフィグレーション表示例 10

```
(config)# show netflow
netflow yes
    sample 2048   ← 妥当な値が設定されていること
    entries 0 4000
    flow-export-version 5
            destination 172.16.178.2 udp 1234
    port 1/1-2
!
(config)#
```

● 収集するポートの PRU に対してエントリ数が設定されていることを確認してください。エントリ数が設定されていないと NetFlow 統計は動作しません。

図 8-26　コンフィグレーション表示例 11

```
(config)# show netflow
netflow yes
    sample 2048
    entries 0 4000  ← 妥当なPRUに対して値が設定されていること
    flow-export-version 5
            destination 172.16.178.2 udp 1234
            port 1/1-2
!
 (config)#
```

(2) インタフェース情報の確認

NetFlow 統計で使用する本装置のインタフェース状態を，show interface コマンドを実行することにより，監視するポートの up/down 状態が”active up”（正常動作中）であることを確認してください。

図 8-27　インタフェース状態表示例

```
> show interface nif 0 line 0
2003/04/02 12:00:00
NIF0: active 1-port 1000BASE-SX retry:2
Average:700/2000Mbps Peak:750Mbps at 10:10:12
Line0:active up 1000BASE-SX full 00:12:E2:45:0a:01
           Protocol:up
           IP address:10.0.0.2 Broadcast IP address:10.0.0.255
(以下省略)
>
```

インタフェースが DOWN 状態の場合は，「8.5.1　通信ができない，または切断されている」を参照してください。

(3) コレクタ装置との通信の確認

NetFlow 統計で使用するコレクタ装置との通信が確立されているか，コマンドラインから ping コマンドを実行することにより確認してください。

図 8-28　コレクタ装置との通信確認例

```
> ping 192.1.1.1
pinging 192.1.1.1 with 32 bytes of data:

reply from 192.1.1.1: bytes=32 time<10ms TTL=128
reply from 192.1.1.1: bytes=32 time<10ms TTL=128
reply from 192.1.1.1: bytes=32 time<10ms TTL=128
reply from 192.1.1.1: bytes=32 time<10ms TTL=128

Ping statistics for 192.1.1.1:
    Packet: Sent = 4, Received = 4,Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
>
```

8.14.5　フロー単位統計パケットがコレクタに届かない (NetFlow 統計)

次に示す手順で確認してください。

- コンフィグレーションにフロー単位統計パケットの送信先であるコレクタ装置の IP アドレスと UDP ポート番号が正しく設定されていることを確認してください。

図 8-29 コンフィグレーション表示例 12

```
(config)# show netflow
netflow yes
    sample 2048
    entries 0 4000
    flow-export-version 5
           destination 172.16.178.2 udp 1234 ← コレクタ情報が正しく設定されていること
    port 1/1-2
!
(config)#
```

8.14.6 フロー集約統計パケットがコレクタに届かない (NetFlow 統計)

次に示す手順で確認してください。

● コンフィグレーションにフロー集約統計の送信先であるコレクタ装置の IP アドレスと UDP ポート番号が正しく設定されていることを確認してください。

図 8-30 コンフィグレーション表示例 13

```
(config)# show netflow
netflow yes
    sample 2048
    entries 0 4000
    flow-aggregation-cache prefix
             aggregation-entries 16000
             mask-source-minimum 24
             mask-destination-minimum 24
             destination 192.1.1.12 ← コレクタ情報が正しく設定されていること
    port 1/1-2
!
(config)#
```

● コンフィグレーションでフロー単位統計のタイムアウト値 (timeout-inactive) がフロー集約統計のタイムアウト値より小さいことを確認してください。以下の例ではフロー集約統計のタイムアウト値 (timeout-inactive)30 秒からフロー単位統計とフロー集約統計のタイムアウト値の合計である 630 秒までの間隔で通知される可能性があります。

図 8-31 コンフィグレーション表示例 14

```
(config)# show netflow
netflow yes
    sample 2048
    entries 0 4000
    flow-export-version 5
             timeout-active 20
             timeout-inactive 600 ← 大きな値が入っていませんか?
             destination 172.16.178.2 udp 1234
    flow-aggregation-cache prefix
             aggregation-entries 16000
             timeout-inactive 30
             mask-source-minimum 24
             mask-destination-minimum 24
             destination 192.1.1.12
port 1/1-2
!
(config)#
```

8.14.7 フロー統計パケット (NetFlow Version 9) がコレクタに届かない【OP-ADV】

次に示す手順で確認してください。

● コンフィグレーション flow-export-version に”9”が正しく設定されていることを確認してください。

図 8-32　コンフィグレーション表示例 15

```
(config)# show netflow
netflow yes
   sample 2048
   entries 0 4000
   flow-export-version 9          ←9が設定されていますか？
           timeout-active 20
           timeout-inactive 600
           destination 172.16.178.2 udp 1234
   flow-aggregation-cache prefix
           aggregation-entries 16000
           mask-source-minimum 24
           mask-destination-minimum 24
           ipv6-mask-source-minimum 64
           ipv6-mask-destination-minimum 64
           destination 192.1.1.12
port 1/1-2
!
(config)#
```

● フロー単位統計やフロー集約統計のコンフィグレーションに，コレクタ装置の IP アドレスと UDP ポート番号等のパラメータが正しく設定されていることを確認してください。

図 8-33　コンフィグレーション表示例 16

```
(config)# show netflow
netflow yes
   sample 2048
   entries 0 4000
   flow-export-version 9
           timeout-inactive 600
           destination 172.16.178.2 udp 1234
   flow-aggregation-cache bgp-nexthop-tos          パラメータが漏れていませんか？
           aggregation-entries 16000
           timeout-inactive 30
           destination 192.1.1.12
port 1/1-2
!
(config)#
```

8.14.8　PRU 単位のフロー統計情報が見えない

次に示す手順で確認してください。

● コンフィグレーションにエントリ数が設定されていることを確認してください。

図 8-34　コンフィグレーション表示例 17

```
(config)# show netflow
netflow yes
   sample 2048
   entries 0 1000  ← NetFlow統計を行いたいPRU番号が設定されていること
   flow-export-version 5
       destination 172.16.178.2 udp 1234
   port 1/1-2
!
(config)#
```

図 8-35　show netflow コマンドの実行結果

```
> show netflow
Progress time from NetFlow statistics cleared:  0:02:56
PRU0: Active
  Received Flows      :          0  Dropped Flows       :          0
  Overflow Entries    :          0
  Used Entries        :          0  Un-used Entries     :       1000
PRU1: Active(No Entry)    ←No Entryが表示されていませんか？
  Received Flows      :          0  Dropped Flows       :          0
  Overflow Entries    :          0
  Used Entries        :          0  Un-used Entries     :          0
Flow export Version: 5,  Service status: enable
  Active Timeout: 30 minutes,  Inactive Timeout: 15 seconds
  Collector: 172.16.178.2 udp: 1234,  Source: 10.1.1.10
  Send Flows          :          0  Discard Flows       :          0
  Send UDP Packets    :          0  Discard UDP Packets :          0
   (以下省略)
```

● PRU の状態を確認してください。

図 8-36　show pru information コマンドの実行結果

```
> show pru information
2005/02/01 13:58:56
PRU 0 : disconnected    ←運用停止中になっていませんか？
PRU 1 : PRU-B2 connected                    average:   0%
        Corrected RCAM data:          0    Corrected FCAM data:          0
PRU 2 : disconnected
PRU 3 : disconnected
```

● 使用エントリ数を確認してください。

図 8-37　show flow used_resources shared_qos コマンドの実行結果

```
(config)# show flow used_resources shared_qos
Used resources in system
    Total: 16000  Free:  4000 ←— NetFlow統計で使用しているエントリ数が基本制御機構
                                  のエントリ数制限をオーバーしていませんか？
Used resources in PRU
    PRU No.    qos   NetFlow   ( free )
         0       0    10000    (  6000)
         1    2000     4000 ←  ( 10000)  PRU当たりの使用エントリ数がPRU種別によるエントリ
         2       0        0    ( 16000)  数制限をオーバーしていませんか？
         3       0        0    ( 16000)
 (config)#
```

図 8-38　コンフィグレーション表示例 18

```
(config)# show netflow
netflow yes
   sample 2048
   entries 0 10000
   entries 1 4000
   flow-export-version 5
       destination 172.16.178.2 udp 1234
   port 1/1-2
!
(config)#
```

Used resource in system における使用可能エントリ数は，BCU 搭載メモリ量によって変わります。詳細については，SB-7800R の場合，「解説書 Vol.1　3.2.1 SB-7800R の収容条件」の「解説書 Vol.1　3.2.1(4) 基本制御モジュール (BCU) のメモリ量と収容経路エントリ数」を参照してください。

Used resource in PRU における使用可能エントリ数については，SB-7800R の場合，「解説書 Vol.1　3.2.1 SB-7800R の収容条件」の「解説書 Vol.1　3.2.1(11)(d) NetFlow 統計のエントリ数」を参照してください。

8.15 隣接装置管理機能の通信障害

8.15.1 LLDP 機能により隣接装置情報が取得できない

LLDP 機能で隣接装置の情報が正しく取得できない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 8-34 LLDP 機能使用時の障害解析方法

項番	確認内容・コマンド	対応
1	show lldp コマンドを実行し，LLDP 機能の動作状態を確認してください。	Enabled の場合は項番 2 へ。
		Disabled の場合は LLDP 機能が停止状態となっています。コンフィグレーションを確認してください。
2	show lldp コマンドを実行し，ポート情報を確認してください。	該当するポート情報が表示されている場合は項番 3 へ。
		該当するポートが表示されていない場合は LLDP 機能の動作対象外となっています。コンフィグレーションを確認してください。
3	show lldp コマンドを実行し，ポート状態を確認してください。	Up 状態の場合は項番 4 へ。
		Down 状態の場合は回線状態を確認してください。確認方法は「8.4 ネットワークインタフェースの通信障害」を参照してください。
4	show lldp コマンドを実行し，隣接装置情報数を確認してください。	0 以外の場合は項番 5 へ。
		0 の場合は隣接装置側で項番 1 から項番 4 を調査してください。隣接装置側でも隣接装置情報数が 0 の場合は，装置間の接続が誤っている可能性があるため，接続を確認してください
5	show lldp コマンドを本装置および隣接装置で実行し，以下が一致しているかを確認してください。 • 本装置側の表示結果で隣接情報中の Chassis ID • 隣接装置の Chassis ID	一致する場合は項番 6 へ。
		不一致の場合は接続先の装置が想定している装置と異なります。ネットワーク構成を確認してください。
6	show lldp コマンドを本装置および隣接装置で実行し，以下が一致しているかを確認してください。 • 本装置側の表示結果で隣接情報中の Port ID • 隣接装置の Port ID	一致する場合は該当ポート間で接続されています。ネットワーク構成上で問題ある場合はネットワーク管理者に連絡してください。
		不一致の場合は隣接装置間で別の回線に接続されています。接続を確認してください。

8.15.2 OADP 機能により隣接装置情報が取得できない

OADP 機能で隣接装置の情報が正しく取得できない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 8-35　OADP 機能使用時の障害解析方法

項番	確認内容・コマンド	対応
1	show oadp コマンドを実行し，OADP Status の表示を確認してください。	Enabled の場合は項番 2 へ。
		Disabled の場合は OADP 機能が停止状態となっています。コンフィグレーションを確認してください。
2	show oadp コマンドを実行し，Enabled Port の表示を確認してください。	該当するポート情報が表示されている場合は項番 3 へ。
		該当するポートが表示されていない場合は OADP 機能の動作対象外となっています。コンフィグレーションを確認してください。
3	show interfaces コマンドを実行し，ポートの状態を確認してください。	該当するポートの状態が active up の場合は項番 4 へ。
		その他の場合は「8.4　ネットワークインタフェースの通信障害」を参照してください。
4	show oadp コマンドを実行し，該当するポートの隣接装置情報を確認してください。	表示されない場合は隣接装置側で項番 1 から項番 4 を調査してください。隣接装置側でも該当ポートの隣接装置情報が表示されない場合は，装置間の接続が誤っている可能性があるため，接続を確認してください

8.16 NTP の通信障害

8.16.1 NTP による時刻同期ができない

NTP による時刻同期ができない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 8-36 NTP の障害解析方法

項番	確認内容・コマンド	対応
1	コンフィグレーションでタイムゾーンの定義があることを確認してください。	コンフィグレーションにタイムゾーンが定義されている場合は項番 2 へ。
		コンフィグレーションにタイムゾーンが定義されていない場合はタイムゾーンの定義をしてください。
2	タイムゾーンコンフィグレーションが反映されているか show calendar コマンドで確認してください。	コマンドの表示結果にタイムゾーンの情報が含まれている場合は項番 3 へ。
		コマンドの表示結果にタイムゾーンの情報が含まれていない場合は，装置を再起動してタイムゾーンの情報を反映させてください。
3	本装置と NTP サーバとの時刻差を確認してください。	本装置と NTP サーバとの時刻差が 1000 秒以内の場合は項番 4 へ。
		本装置と NTP サーバとの時刻差が 1000 秒以上ある場合には，set calendar コマンドを使用して本装置の時刻を NTP サーバと合わせてください。
4	NTP サーバとの IPv4 による通信を確認してください。	NTP サーバと本装置間で IPv4 の通信が可能か，ping コマンドで確認してください。
		NTP サーバの設定で，UDP ポート番号 123 のパケットを廃棄する設定がないことを確認してください。

9 保守作業

この章では，主に保守関連作業を行うときの作業手順について説明しています。

9.1　障害情報の取得

show tech-support コマンドを使用して，障害発生時の情報採取を一括して採取できます。また，本コマンドでは，採取した障害情報を指定した ftp サーバに転送できます（「9.2.3　show tech-support コマンドを使用した保守情報のファイル転送」を参照)。本コマンドで採取する情報を次の表に示します。

表 9-1　show tech-support コマンドの情報採取内容

情報採取レベル※	採取内容
基本情報	ソフトウェアバージョン情報
	ハードウェア実装情報
	運用系，待機系のログ情報，ダンプ情報
	インタフェース情報
	統計情報
	MC 情報
	コンフィグレーション（コマンドオプションで採取しないことも可能です）
	プロセス情報
	バッファ情報
詳細情報	インタフェース詳細情報
	ハードウェアバッファ情報
	経路情報統計
	フィルタ情報
	QoS 情報
	SNMP のソフトウェア動作情報
	その他，ソフトウェア，ハードウェアの障害トレース情報

注※　show tech-support コマンドに detail パラメータを付けて実行した場合は「基本情報」と「詳細情報」を採取し，detail パラメータを付けないで実行した場合は「基本情報」だけを採取します。

9.1.1　運用端末から ftp コマンドを使用した障害情報の取得

(1)　リモート運用端末から障害情報を取得する

表 9-2　ftp コマンドで取得できる情報

項番	get 指定ファイル名	取得情報
1	.show-tech	show tech-support の表示結果
2	.show-tech-detail	show tech-support detail の表示結果

図 9-1 リモート運用端末からの障害情報の取得

```
基本情報の取得
client-host >ftp sb7800r             <-ftpクライアントから
sb7800rにftp接続
Connected to sb7800r.
220  FTP server (Version wu-2.4(1) Tue Apr 1 15:33:09 JST 2003) ready.
User (sb7800r:(none)): staff1
331 Password required for staff1.
Password:****
230 User staff1 logged in.
ftp> get .show-tech show-tech.txt              <-.show-techファイルの転送
200 PORT command successful.
150 Opening ASCII mode data connection for /etc/ftpshowtech.
226 Transfer complete.
ftp: 142533 bytes received in 2.56Seconds 55.61Kbytes/sec.
ftp> quit
221 Goodbye.
client-host>
クライアントホストにshow-tech.txtファイルが取得されます。

詳細情報の取得
client-host >ftp sb7800r             <-ftpクライアントから
sb7800rにftp接続
Connected to sb7800r.
220  FTP server (Version wu-2.4(1) Tue Apr 1 15:33:09 JST 2003) ready.
User (sb7800r:(none)): staff1
331 Password required for staff1.
Password:****
230 User staff1 logged in.
ftp> get .show-tech-detail show-tech-detail.txt
    <-.show-tech-detailファイルの転送
200 PORT command successful.
150 Opening ASCII mode data connection for /etc/ftpshowtech.
226 Transfer complete.
ftp: 273603 bytes received in 29.56Seconds 9.26Kbytes/sec.
ftp> qui
221 Goodbye.
client-host>
クライアントホストにshow-tech-detail.txtファイルが取得されます。
```

注

- ftp の ls などのコマンドで，get 指定すべきファイルは見えないので，事前のファイルの容量確認等はできません。
- 本情報の取得時は，SB-7800R 側でコマンドを実行するため，転送中の状態が長く続きますが，途中で転送を中断しないでください。
- SB-7800R の負荷状態や通信路の状態によっては，クライアント側がネットワークタイムアウトで切断することがあります。その場合は，クライアントのタイムアウト時間を長く設定してください。
- ftp での障害情報取得では show running-config コマンドなど，装置管理者モードでだけ実行できるコマンドの実行結果は採取しません (/config/system.cnf の内容は採取します)。
- show tech-support を取得したときに，ログ情報に残るユーザ名は ftpuser となります。

9.2　保守情報のファイル転送

装置運用中に障害発生により自動的に採取されたログ情報やダンプ情報，またはコマンドを用いることで採取したダンプ情報をコンソールまたはリモート運用端末にファイル転送する方法を示します。ファイル転送を行うには ftp コマンド，zmodem コマンド，および show tech-support コマンドの三つの方法があります。なお，保守情報には次の表に示すものがあります。

表 9-3　保守情報

項番	項目	格納場所およびファイル名
1	装置再起動時のダンプ情報ファイル	/primaryMC/var/dump/rmdump
2	CP および PRU，NIF，イベントのダンプ情報ファイル	/primaryMC/var/dump/cp00.***　... 標準の CP ダンプ /secondaryMC/var/dump/cp00e1.*** ... 拡張の CP ダンプ（拡張の CP ダンプ採取指定時だけ） /primaryMC/var/dump/pru**.***　... 標準の PRU ダンプ /secondaryMC/var/dump/pru**e1.*** ... 拡張の PRU ダンプ（拡張の PRU ダンプ採取指定時だけ） /primaryMC/var/dump/nif**.***　...NIF ダンプ (** はスロット番号，*** はシーケンス番号または”cmd”) /primaryMC/usr/var/evtdump/cpevt +++.*** ... イベントダンプ (+++ はイベント番号 (「表 8-6　イベントダンプ採取イベント一覧」参照)，*** はシーケンス番号)
3	ログ情報	採取したディレクトリ（「図 9-3　ログ情報のリモート運用端末へのファイル転送」を参照）から次の名前で格納する 運用ログ :log.txt 種別ログ：log_ref.txt
4	コンフィグレーションファイル	/config/system.cnf
5	障害待避情報	/primaryMC/var/core/*.core

注 1
　項番 1，2 および 5 のファイルを ftp コマンドで転送する場合はバイナリモードで転送してください。

注 2
　拡張の CP ダンプを指定した場合，標準の CP ダンプと拡張の CP ダンプの，二つのダンプファイルを出力します。拡張の PRU ダンプを指定した場合，標準の PRU ダンプと拡張の PRU ダンプの，二つのダンプファイルを出力します。

注 3　系切替中の PRU 障害発生時はダンプ情報が採取されません。

9.2.1　ftp コマンドを使用したファイル転送

リモート運用端末との間でファイル転送を行う場合は ftp コマンドを使用します。

(1) ダンププファイルをリモート運用端末に転送する

図 9-2　ダンプファイルのリモート運用端末へのファイル転送

```
> cd /var/dump/
> ftp 192.168.0.1 <------------------------ 転送先端末のアドレスを指定
Connect to 192.168.0.1.
220  FTP server (Version wn-2.4(4) Fri Jan 1 00:00:00 JST 1999) ready.
Name (192.168.0.1:operator): test
331 Password required for test.
Password:xxxxxx
230 User test logged in.
Remote system type UNIX.
Using binary mode to transfer files.
ftp>prompt <------------------------------ 対話モードを変更
Interactive mode off.
ftp>bin <--------------------------------- バイナリモードに設定※
200 Type set to I.
ftp>cd 転送先ディレクトリ <--------------- 転送先ディレクトリの指定
250 CMD command successful.
ftp> mput * <----------------------------- ダンプファイルの転送
local: rmdump remote: rmdump
200 PORT command successful.
150 Opening BINARY mode data connection for rmdump (2,312,345 bytes)
226 Transfer complete.
local: rp00.000 remote: rp00.000
200 PORT command successful.
150 Opening BINARY mode data connection for rp00.000 (512,322 bytes)
226 Transfer complete.
ftp> bye
221 Goodby
>
```

注※　ダンプファイルは必ずバイナリモードで転送してください。ダンプファイルをアスキーモードで転送すると，正確なダンプ情報が取得できなくなります。

(2) ログ情報をリモート運用端末に転送する

図 9-3 ログ情報のリモート運用端末へのファイル転送

```
> show logging > log.txt
> show logging reference > log_ref.txt
> ftp 192.168.0.1 <―――――――――――――― 転送先端末のアドレスを指定
Connect to 192.168.0.1.
220  FTP server (Version wn-2.4(4) Fri Jan 1 00:00:00 JST 1999) ready.
Name (192.168.0.1:operator): test
331 Password required for test.
Password:xxxxxx
230 User test logged in.
Remote system type UNIX.
Using binary mode to transfer files.
ftp>ascii <―――――――――――――――――― アスキーモードに設定
200 Type set to A.
ftp>cd 転送先ディレクトリ <――――――――― 転送先ディレクトリの指定
250 CMD command successful.
ftp> put log.txt <―――――――――――――― ログ情報の転送
local: log.txt remote: log.txt
200 PORT command successful.
150 Opening ASCII mode data connection for log.txt (1,345 bytes)
226 Transfer complete.
ftp>put log_ref.txt
local: log_ref.txt remote: log_ref.txt
200 PORT command successful.
150 Opening ASCII mode data connection for log_ref.txt (846 bytes)
226 Transfer complete.
ftp> bye
221 Goodby
>
```

(3) 障害退避情報ファイルをリモート運用端末に転送する

図 9-4　障害退避情報ファイルのリモート運用端末へのファイル転送

```
> cd /primaryMC/var/core
> ls <――――――――――――――――― 障害退避情報ファイルが存在することを確認
interfaceControl.core    nodeInit.core   ファイルが存在しない場合は，何もしないで終了
>
> ftp 192.168.0.1 <――――――――――― 転送先端末のアドレスを指定
Connect to 192.168.0.1.
220  FTP server (Version wn-2.4(4) Fri Jan 1 00:00:00 JST 1999) ready.
Name (192.168.0.1:operator): test
331 Password required for test.
Password:xxxxxx
230 User test logged in.
Remote system type UNIX.
Using binary mode to transfer files.
ftp>prompt <――――――――――――― 対話モードを変更
Interactive mode off.
ftp>bin <―――――――――――――― バイナリモードに設定※
200 Type set to I.
ftp>cd 転送先ディレクトリ <―――――― 転送先ディレクトリの指定
250 CMD command successful.
ftp> mput *.core <――――――――――― 障害退避情報ファイルの転送
local: interfaceControl.core remote: interfaceControl.core
200 PORT command successful.
150 Opening BINARY mode data connection for interfaceControl.core, (16,363 bytes)
226 Transfer complete.
local: nodeInit.core remote: nodeInit.core
200 PORT command successful.
150 Opening BINARY mode data connection for nodeInit.core (29,322 bytes)
226 Transfer complete.
ftp> bye
221 Goodby
>
```

注※　障害退避情報ファイルは必ずバイナリモードで転送してください。障害退避情報ファイルをアスキーモードで転送すると，正確な障害退避情報が取得できなくなります。

9.2.2　zmodem コマンドを使用したファイル転送

本装置と RS232C ケーブルで接続されているコンソールとの間でファイル転送を行う場合は zmodem コマンドを使用します。なお，通信を始めるに当たり，あらかじめコンソール側通信プログラムの受信操作を行ってください。

(1) ダンプファイルをコンソールに転送する

図 9-5　ダンプファイルのコンソールへのファイル転送

```
> cd /var/dump/
> zmodem put rmdump <―――――――― ダンプファイルの転送
**000000000000
>
```

(2) ログ情報をコンソールに転送する

図 9-6 ログファイルのコンソールへのファイル転送

```
> show logging > log.txt
> show logging reference > log_ref.txt
> zmodem put log.txt  <-------------------  ログファイルの転送
**000000000000
> zmodem put log_ref.txt
**000000000000
>
```

(3) 障害退避情報ファイルをコンソールに転送する

図 9-7 障害退避情報ファイルのコンソールへのファイル転送

```
> cd /primaryMC/var/core
> ls <--------------------------------- 障害退避情報ファイルが存在することを確認
interfaceControl.core   nodeInit.core   ファイルが存在しない場合は，何もしないで終了
> zmodem put interfaceControl.core <--- ログファイルの転送
**000000000000
> zmodem put nodeInit.core
**000000000000
>
```

9.2.3 show tech-support コマンドを使用した保守情報のファイル転送

リモート運用端末またはリモートホストに対して保守情報のファイル転送を行う場合は show tech-support コマンドを使用します。

(1) 保守情報をリモート運用端末またはリモートホストに転送する

図 9-8 保守情報のリモート運用端末またはリモートホストへのファイル転送

```
> show tech-support ftp                                              <-  ※1
Specify Host Name of FTP Server.       : ftpserver.example.com       <-  ※2
Specify User ID for FTP connections.   : user1                       <-  ※3
Specify Password for FTP connections.  : xxxxxx                      <-  ※4
Specify Path Name on FTP Server.       : /usr/home/user1             <-  ※5
Specify File Name of log and Dump files: support                     <-  ※6
Transfer Text file
file name      support.txt
Executing . . . . . . . . . . . . .
Operation normal end.
########## Dump files' Information ##########
***** ls -l /dump0 *****
total 1368
-rwxr-xr-x  1 root  wheel  1316167 Apr 23 21:14 rmdump
-rwxr-xr-x  1 root  wheel    52077 Apr 23 21:14 dpdump
***** ls -l /standby/dump0 *****
total 1368
-rwxr-xr-x  1 root  wheel  1316167 Apr 23 21:14 rmdump
-rwxr-xr-x  1 root  wheel    52077 Apr 23 21:14 dpdump
########## End of Dump files' Information ##########
########## Core files' Information ##########
***** ls -l /primaryMC/usr/var/core *****
***** ls -l /standby/primaryMC/usr/var/core *****
No Core Files
########## End of Core files' Information ##########
Transfer binary file
file name      support.tgz
Executing . . . . . . . . . . . . . .
Operation normal end.
>
```

注※1 コマンドの実行
注※2 リモートホスト名を指定
注※3 ユーザ名を指定
注※4 パスワードを入力
注※5 転送先ディレクトリの指定
注※6 ファイル名を指定

9.2.4 運用端末から ftp コマンドを使用したファイル転送

(1) リモート運用端末からダンプ情報ファイルを取得する

表 9-4 ftp コマンドで取得できるファイル

項番	get 指定ファイル名	取得ファイル
1	.dump	/dump0 と /dump1 以下のファイル（圧縮）
2	.dump0	/dump0 以下のファイル（圧縮）
3	.dump1	/dump1 以下のファイル（圧縮）

図 9-9 リモート運用端末からのダンプファイルの取得

```
client-host >ftp sb7800r            <-ftpクライアントからsb7800rにftp接続
Connected to sb7800r.
220  FTP server (Version wu-2.4(1) Tue Apr 1 15:33:09 JST 2003) ready.
User (sb7800r:(none)): staff1
331 Password required for staff1.
Password:****
230 User staff1 logged in.
Remote system type Is UNIX.
ftp> binary                                         <-  ※1
200 Type set to I.
ftp> get .dump dump.tgz                             <-ダンプファイルの転送
200 PORT command successful.
150 Opening BINARY mode data connection for /etc/ftpdump.
226 Transfer complete.
ftp: 4478793 bytes received in 15.66Seconds 286.08Kbytes/sec.
ftp> quit
221 Goodbye.
client-host>
クライアントホストにdump.tgzファイルが取得されます。
```

注※ 1

ダンプ情報ファイルは必ずバイナリモードで転送してください。アスキーモードでは転送できません。

注

- ftp の ls などのコマンドで，get 指定すべきファイルは見えないので，事前のファイルの容量確認等はできません。
- SB-7800R の負荷状態や通信路の状態によっては，クライアント側がネットワークタイムアウトで切断することがあります。その場合は，クライアントのタイムアウト時間を長く設定してください。

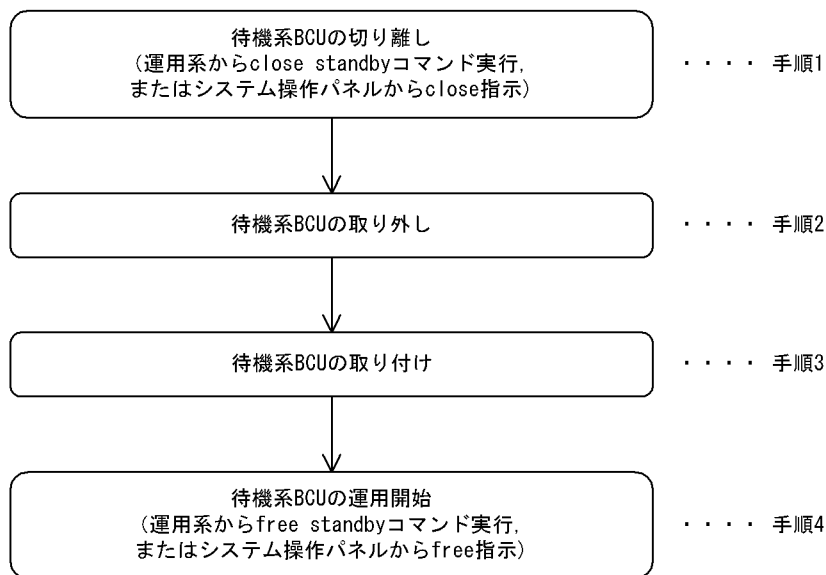
9.3 障害が発生したボードの交換

9.3.1 障害が発生したボードの交換（電源 ON したまま）

ここでは本装置の BCU，PRU，PRU 内蔵型高密度ポート NIF，NIF で障害が発生して，ボードの交換が必要なときの手順を記載しています。交換対象となるボードに応じて，次に記載してある説明を参照してください。なお，各ボードの搭載位置に関する説明および LED に関する説明は「ハードウェア取扱説明書」を参照してください。

(1) 運用中なので電源 ON したまま，待機系 BCU を交換したい

電源 ON したまま待機系 BCU を交換する概略手順を次の図に示します。

図 9-10　待機系 BCU 交換手順

次に各手順の詳細を記載します。

(手順 1) 待機系 BCU の切り離し

まず，運用系 BCU に接続した運用端末から，次に示す show system コマンドを実行して，待機系 BCU の運用状態を確認してください。

```
> show system [Enter]
```

コマンド実行結果を次の図に示します（次の図では「BCU0」が運用系，「BCU1」が待機系となっています)。

図 9-11 show system コマンド実行結果

```
> show system
System : SB-7808R, SB-780S-R Ver. 9.2 [OS-R]
Node : Name=System Name
    Contact=Contact Address
    Locate=Location
     :       :       :       :       :       :
    BCU0 : Active
        RM-CPU : Active SB-BCU-RM8MS[BCU-RM8MS]
        Boot : 2003/01/11 19:27:42 , Power ON , 0 times restart
     :       :       :       :       :       :
    BCU1 : Fault ◀──────────────── 待機系BCUの運用状態
     :       :       :       :       :       :
```

＜待機系 BCU が障害になっている場合＞

待機系 BCU が障害になっている場合，待機系 BCU の状態が「Fault」になっています。この場合，運用系 BCU に接続した運用端末から，次に示す待機系 BCU を閉塞状態にする close standby コマンドを実行してください。

```
> close standby [Enter]
```

システム操作パネルから運用停止させることもできます。この場合，次のとおり操作してください。

<Main Menu>→”Action”⇒<ACTION>→”CLOSE”⇒”standby”を選択

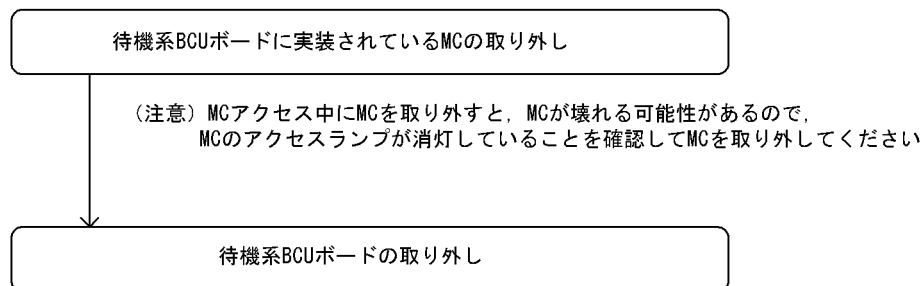
本コマンド，または本操作を実行後，(手順 2) に従って待機系 BCU を取り外してください。

＜待機系 BCU が障害になっていない場合＞

障害の発生した BCU が再立ち上げに成功した場合，待機系 BCU の状態が「Standby」になっています。この場合にも，再発防止の観点から BCU ボードを交換することをお勧めします。

(手順 2) 待機系 BCU の取り外し

待機系 BCU の取り外し手順を次の図に示します。

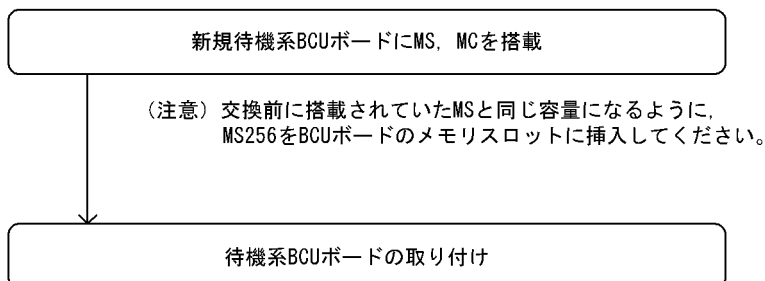
図 9-12 待機系 BCU 取り外し手順

〔注意事項〕

感電する恐れがあります。電源を ON したままでのボードの取り外し／取り付け作業は，教育を受けた技術者または保守員に依頼してください。

（手順 3）待機系 BCU の取り付け

＜交換対象が待機系 BCU の場合＞

待機系 BCU の取り付け手順を次の図に示します。なお，待機系 BCU の取り付け手順は，（手順 2）で説明した取り外し手順とは一部順序が異なっているで注意してください。

図 9-13　待機系 BCU 取り付け手順

〔注意事項〕

感電する恐れがあります。電源を ON したままでのボードの取り外し／取り付け作業は，教育を受けた技術者または保守員にご依頼ください。

（手順 4）待機系 BCU の運用開始

待機系 BCU を交換しただけでは，待機系 BCU は運用状態（正常な二重化運用）になりません。（手順 3）終了後，運用系 BCU に接続した運用端末から，次に示す待機系 BCU を運用状態にする free standby コマンドの実行が必要です。

```
> free standby [Enter]
```

システム操作パネルから運用開始させることもできます。この場合，次のとおり操作してください。

<Main Menu>→”Action”⇒<ACTION>→”FREE”⇒”standby”を選択

本コマンド，または本操作を実行後，待機系 BCU の運用状態が「Standby」になっていることを確認してください。待機系 BCU の運用状態の確認方法は，運用系に接続した運用端末から，次に示す show system コマンドを実行してください。

```
> show system [Enter]
```

show system コマンド実行結果を次の図に示します。

図 9-14 show system コマンド実行結果

```
> show system
System : SB-7808R, SB-780S-R Ver. 9.2 [OS-R]
Node : Name=System Name
    Contact=Contact Address
    Locate=Location
     :       :       :       :       :       :
    BCU0 : Active
        RM-CPU : Active SB-BCU-RM8MS[BCU-RM8MS]
        Boot : 2003/01/11 19:27:42 , Power ON , 0 times restart
     :       :       :       :       :       :
    BCU1 : Standby  <------  待機系BCUの運用状態が「standby」であること
        RM-CPU : Active SB-BCU-RM8MS[BCU-RM8MS]
        Boot : 2003/01/11 19:27:43 , Power ON , 0 times restart
     :       :       :       :       :       :
```

〔交換後の注意事項〕

スロット 0，スロット 1 両方の MC スロットに MC を実装している場合，BCU 交換後の初期状態ではスロット 0 の MC を優先して起動するように設定されています。このため，待機系 BCU 交換前に set mode コマンドによりスロット 1 の MC を優先して起動する設定で運用していて，待機系 BCU 交換後も同様にスロット 1 の MC を優先して起動したい場合は，運用系 BCU に接続した運用端末から，装置管理者モードに移行したあと，次に示す set mode コマンドで再度設定してください。

```
# set mode standby slot1 reload [Enter]
```

待機系 BCU 起動時の優先 MC スロットの設定後，運用系 BCU に接続した運用端末から，次に示す reload コマンドにより，待機系 BCU を再起動してください。なお，本コマンドは，装置管理者モードでなくても実行できます。

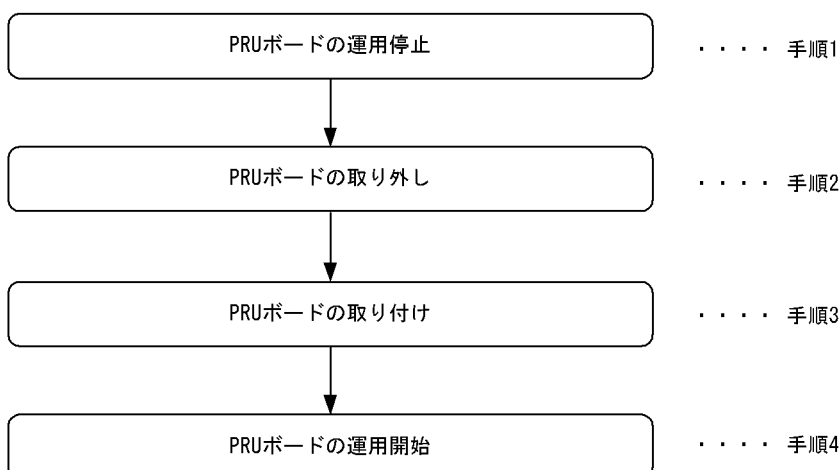
```
> reload dump-image -f standby [Enter]
```

待機系 BCU 再起動後，待機系 BCU の運用状態が「Standby」になっていることを確認してください。待機系 BCU の運用状態の確認方法は，運用系 BCU に接続した運用端末から，次に示す show system コマンドを実行してください。show system コマンドの実行結果は，「図 9-14　show system コマンド実行結果」を参照してください。

```
> show system [Enter]
```

(2) 運用中なので電源 ON したまま，PRU を交換したい

電源 ON したまま PRU を交換する概略手順を次の図に示します。

図 9-15 PRU ボード取り外し手順

次に各手順の詳細を記載します。

（手順 1）PRU ボードの運用停止

撤去する PRU の運用を停止します。次に示す close pru コマンドを運用端末から実行します。このとき，対象となる PRU 配下の NIF は運用中であっても停止します。

close [-f] pru <PRU No.>[Enter]　（ PRU No.：対象となるPRU番号）

システム操作パネルから運用停止させることもできます。この場合，次のとおり操作してください。

<Main Menu>→”Action”⇒<ACTION>→”CLOSE”⇒”PRUx”　(x ： 対象となるPRU番号)を選択

（手順 2）PRU ボードの取り外し

対象となる PRU ボードの STATUS LED 表示が消灯していることを確認したあと，対象となる PRU ボードに取り付けられている NIF ボードを取り出し，次に PRU ボードを取り外してください。詳細は，「ハードウェア取扱説明書」を参照してください。

〔注意事項〕

感電する恐れがあります。電源を ON したままでのボードの取り外し／取り付け作業は，教育を受けた技術者または保守員にご依頼ください。

（手順 3）PRU ボードの取り付け

空きスロットに PRU ボードを取り付けます。次に PRU ボードに（手順 2）で取り外した NIF ボードを取り付けます。詳細は，「ハードウェア取扱説明書」を参照してください。

〔注意事項〕

感電する恐れがあります。電源を ON したままでのボードの取り外し／取り付け作業は，教育を受けた技術者または保守員にご依頼ください。

（手順 4）PRU ボードの運用開始

取り付けた PRU ボードの運用を開始します。次に示す free pru コマンドを運用端末から実行します。

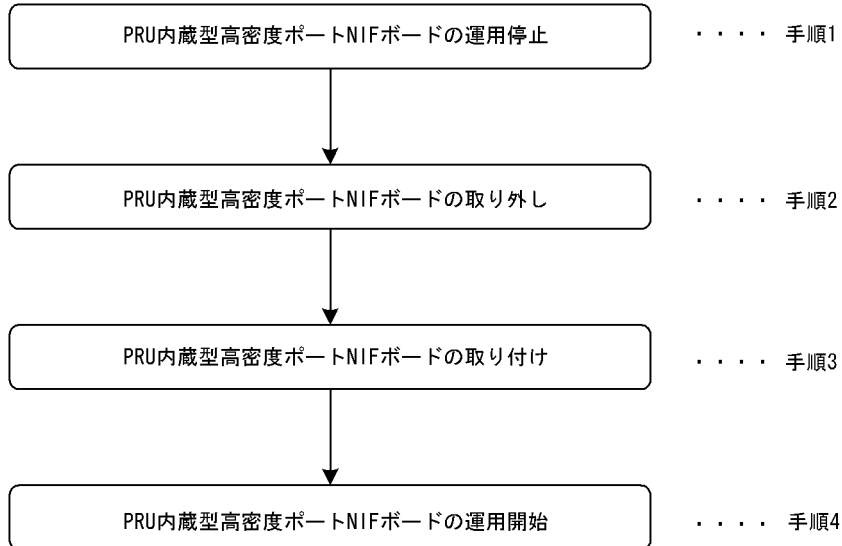
free pru <PRU No.>[Enter]　（ PRU No.：対象となるPRU番号）

システム操作パネルから運用開始させることもできます。この場合，次のとおり操作してください。

<Main Menu>→”Action”⇒<ACTION>→”FREE”⇒”PRUx”　(x ： 対象となるPRU番号)を選択

(3) 運用中なので電源 ON したまま，PRU 内蔵型高密度ポート NIF を交換したい

電源 ON したまま PRU 内蔵型高密度ポート NIF を交換する概略手順を次の図に示します。

図 9-16 PRU 内蔵型高密度ポート NIF ボード取り外し手順

次に各手順の詳細を記載します。

(手順 1) PRU 内蔵型高密度ポート NIF ボードの運用停止

撤去する PRU 内蔵型高密度ポート NIF の運用を停止します。次に示す close pru コマンドを運用端末から実行します。このとき，対象となる PRU 内蔵型高密度ポート NIF 配下の NIF は運用中であっても停止します。

```
close [-f] pru <PRU No.>[Enter]    ( PRU No.：対象となるPRU番号)
```

システム操作パネルから運用停止させることもできます。この場合，次のとおり操作してください。

<Main Menu>→”Action”⇒<ACTION>→”CLOSE”⇒”PRUx” (x : 対象となるPRU番号)を選択

(手順 2) PRU 内蔵型高密度ポート NIF ボードの取り外し

対象となる PRU 内蔵型高密度ポート NIF ボードの STATUS LED 表示が消灯していることを確認したあと，PRU 内蔵型高密度ポート NIF ボードを取り外してください。詳細は，「ハードウェア取扱説明書」を参照してください。

〔注意事項〕

感電する恐れがあります。電源を ON したままでのボードの取り外し／取り付け作業は，教育を受けた技術者または保守員にご依頼ください。

(手順 3) PRU 内蔵型高密度ポート NIF ボードの取り付け

空きスロットに PRU 内蔵型高密度ポート NIF ボードを取り付けます。詳細は，「ハードウェア取扱説明書」を参照してください。

〔注意事項〕

感電する恐れがあります。電源を ON したままでのボードの取り外し／取り付け作業は，教育を受けた技術者または保守員にご依頼ください。

（手順 4）PRU 内蔵型高密度ポート NIF ボードの運用開始

取り付けた PRU 内蔵型高密度ポート NIF ボードの運用を開始します。次に示す free pru コマンドを運用端末から実行します。

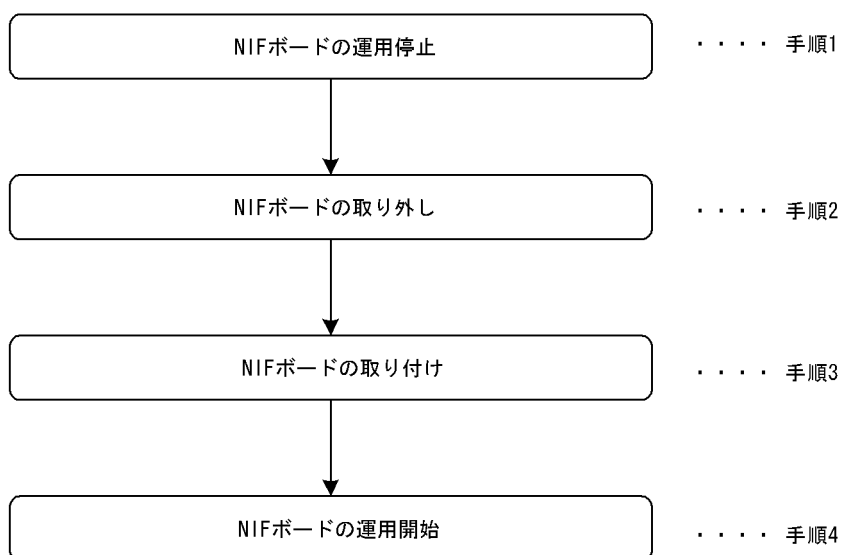
free pru <PRU No.>[Enter]　　（ PRU No.：対象となるPRU番号）

システム操作パネルから運用開始させることもできます。この場合，次のとおり操作してください。

<Main Menu>→”Action”⇒<ACTION>→”FREE”⇒”PRUx” (x : 対象となるPRU番号)を選択

（4） 運用中なので電源 ON したまま，NIF を交換したい

電源 ON したまま NIF を交換する概略手順を次の図に示します。なお，PRU 内蔵型高密度ポート NIF の場合は以下の手順を実行しても，交換はできません。交換方法については，「(3) 運用中なので電源 ON したまま，PRU 内蔵型高密度ポート NIF を交換したい」を参照してください。

図 9-17　NIF ボード取り外し手順

次に各手順の詳細を記載します。

（手順 1）NIF ボードの運用停止

取り外す NIF ボードの運用を停止します。次に示す close nif コマンドを運用端末から実行します。

close [-f] nif <NIF No.>[Enter]　（ NIF No.：対象となるNIF番号）

システム操作パネルから運用停止させることもできます。この場合，次のとおり操作してください。

<Main Menu>→”Action”⇒<ACTION>→”CLOSE”⇒”NIFxx” (xx : 対象となるNIF番号)を選択

（手順 2）NIF ボードの取り外し

対象となる NIF ボードの STATUS LED 表示が消灯していることを確認したあと，NIF ボードを取り外してください。取り外し方法の詳細は，「ハードウェア取扱説明書」を参照してください。

〔注意事項〕

感電する恐れがあります。電源を ON したままでのボードの取り外し／取り付け作業は，教育を受けた技術者または保守員にご依頼ください。

（手順 3）NIF ボードの取り付け

以下の NIF ボード※の場合，取り付け前にインタフェースモードを 8k インタフェースモードに設定してください。詳細については「5.4.1　NE1G-48T の実装手順」を参照してください。
NIF の空きスロットに NIF ボードを挿入します。挿入方法の詳細については，「ハードウェア取扱説明書」を参照してください。
注※　NIF ボード

- NE1G-48T

〔注意事項〕

感電する恐れがあります。電源を ON したままでのボードの取り外し／取り付け作業は，教育を受けた技術者または保守員にご依頼ください。

（手順 4）NIF ボードの運用開始

NIF の付属する PRU ボードが運用状態の場合は，増設した NIF ボードを運用状態にします。次に示す free nif コマンドを運用端末から実行します。

```
free nif <NIF No.>[Enter]     ( NIF No.：対象となるNIF番号)
```

システム操作パネルから運用開始させることもできます。この場合，次のとおり操作してください。

<Main Menu>→”Action”⇒<ACTION>→”FREE”⇒”NIFxx” (xx : 対象となるNIF番号)を選択

NIF の付属する PRU ボードが停止状態の場合，PRU ボードを運用状態にします。次に示す free pru コマンドを運用端末から実行します。PRU が運用状態になると配下の NIF もすべて運用状態になります。

```
free pru <PRU No.>[Enter]     ( PRU No.：対象となるPRU番号)
```

システム操作パネルから運用開始させることもできます。この場合，次のとおり操作してください。

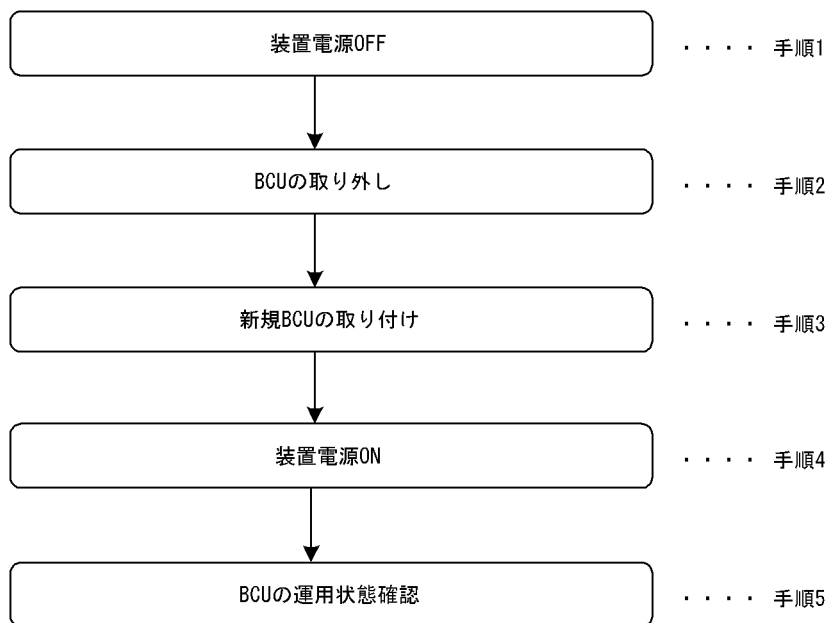
<Main Menu>→”Action”⇒<ACTION>→”FREE”⇒”PRUx” (x : 対象となるPRU番号)を選択

9.3.2　障害が発生したボードの交換（電源 OFF したあと）

ここでは保守点検などでいったん電源 OFF（電源スイッチの搭載位置は，「ハードウェア取扱説明書」を参照）して，ボードを交換する場合の手順を記載しています。

(1) 電源を OFF して BCU を交換したい

電源 OFF の状態で運用系 BCU および待機系 BCU を交換する概略手順を次の図に示します。なお，待機系 BCU の交換は SB-7800R の BCU 二重化サポートモデルだけが該当します。

図 9-18　待機系 BCU 交換手順

次に各手順の詳細説明を記載します。

（手順 1）装置電源 OFF

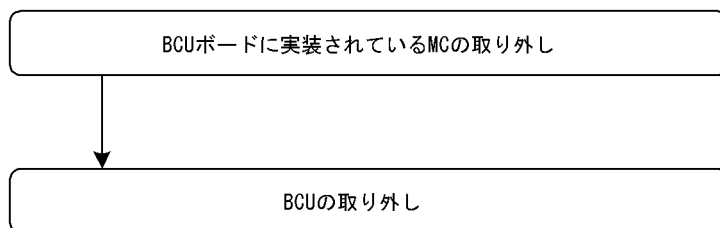
装置の電源を OFF してください。

〔注意事項〕

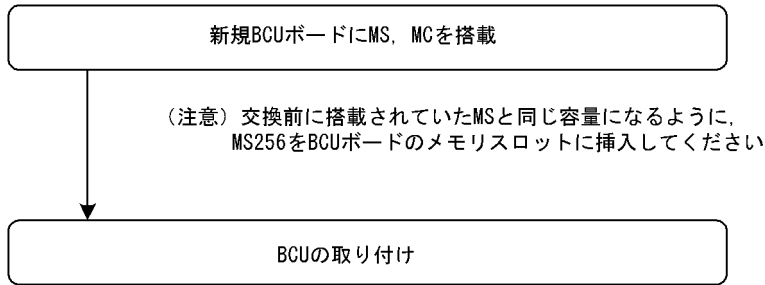
電源冗長化時は，複数の入力電源が供給されています。電源を OFF する場合はすべてのスイッチまたはブレーカを OFF してください。電源 OFF 方法については，「ハードウェア取扱説明書」を参照してください。

（手順 2）BCU の取り外し

BCU の取り外し手順を次の図に示します。

図 9-19　BCU 取り外し手順

（手順 3）新規 BCU の取り付け

新規 BCU の取り付け手順を次の図に示します。

図 9-20　BCU 取り付け手順

（手順 4）装置電源 ON

装置の電源を ON してください。

〔注意事項〕

電源冗長化時は，すべてのスイッチまたはブレーカを ON してください。電源 ON の方法については，「ハードウェア取扱説明書」を参照してください。

（手順 5）BCU の運用状態確認

（手順 4）まで終了して BCU の起動が完了したら，運用系 BCU に接続した運用端末から，次に示す show system コマンドを実行し，待機系 BCU の運用状態が「Standby」であることを確認してください。

```
> show system [Enter]
```

show system コマンド実行結果を次の図に示します。

図 9-21　show system コマンド実行結果

```
> show system
System : SB-7808R, SB-780S-R Ver. 9.2 [OS-R]
Node : Name=System Name
    Contact=Contact Address
    Locate=Location
     :       :       :       :       :       :
    BCU0 : Active                    運用系BCUの運用状態が「ACTIVE」であること
        RM-CPU : Active SB-BCU-RM8MS[BCU-RM8MS]
        Boot : 2003/01/11 19:27:42 , Power ON , 0 times restart
     :       :       :       :       :       :
    BCU1 : Standby                   待機系BCUの運用状態が「standby」であること
        RM-CPU : Active SB-BCU-RM8MS[BCU-RM8MS]
        Boot : 2003/01/11 19:27:43 , Power ON , 0 times restart
     :       :       :       :       :       :
```

〔交換後の注意事項〕

スロット 0，スロット 1 両方の MC スロットに MC を実装している場合，BCU 交換後の初期状態ではスロット 0 の MC を優先して起動するように設定されています。このため，BCU 交換前に set mode コマンドによりスロット 1 の MC を優先して起動する設定で運用していて，BCU 交換後も同様にスロット 1 の MC を優先して起動したい場合は，運用系 BCU に接続した運用端末から，装置管理

者モードに移行したあと，次に示す set mode コマンドで再度設定してください。

```
運用系　# set mode active slot1 reload [Enter]
待機系　# set mode standby slot1 reload [Enter]
```

起動時の優先 MC スロットの設定後，運用系 BCU に接続した運用端末から，次に示す reload コマンドにより，BCU を再起動してください。なお，本コマンドは，装置管理者モードでなくても実行できます。

```
運用系　> reload dump-image -f active [Enter]
待機系　> reload dump-image -f standby [Enter]
```

BCU 再起動後，運用系 BCU に接続した運用端末から，次に示す show system コマンドを実行し，待機系 BCU の運用状態が運用系 BCU の場合は「ACTIVE」，待機系 BCU の場合は「Standby」になっていることを確認してください。show system コマンドの実行結果は，「図 9-21　show system コマンド実行結果」を参照してください。

```
> show system [Enter]
```

(2) 電源 OFF して PRU を交換したい

「ハードウェア取扱説明書」を参照してください。

(3) 電源 OFF して PRU 内蔵型高密度ポート NIF を交換したい

「ハードウェア取扱説明書」を参照してください。

(4) 電源 OFF して NIF を交換したい

「ハードウェア取扱説明書」を参照してください。

〔交換後の注意事項〕

交換する NIF が以下でコンフィグレーションファイルに 16k インタフェースモードが設定されている場合，装置起動後，インタフェースモードを 8k インタフェースモードに変更してください。詳細については，「5.4.1　NE1G-48T の実装手順」を参照してください。

- NE1G-48T

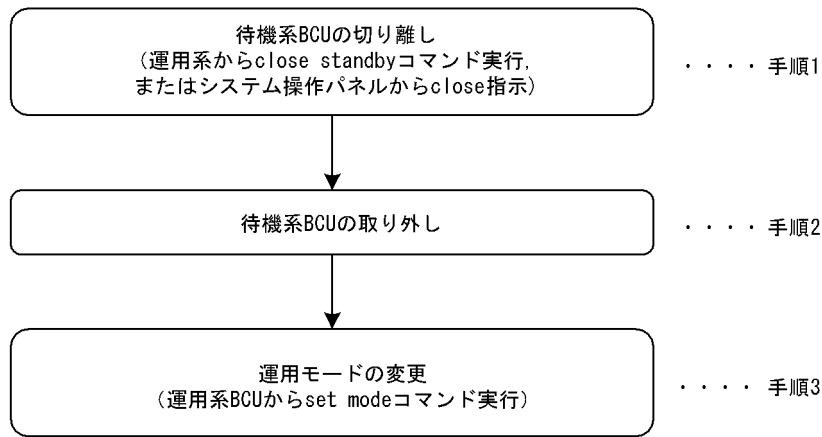
9.4　ボード，メモリの取り外し／増設

9.4.1　ボードの取り外し（電源 ON したまま）

ここでは本装置の BCU，PRU，PRU 内蔵型高密度ポート NIF，NIF で障害が発生したが，ボードの交換品が届くまで取り外しておきたい場合などの手順を記載しています。

(1) 運用中なので電源 ON したまま，待機系 BCU を取り外したい

電源 ON したまま待機系 BCU を取り外す概略手順を次の図に示します。

図 9-22　待機系 BCU 取り外し手順

次に各手順の詳細説明を記載します。

（手順 1）待機系 BCU の切り離し

「9.3.1　障害が発生したボードの交換（電源 ON したまま）（1）運用中なので電源 ON したまま，待機系 BCU を交換したい　**（手順 1）待機系 BCU の切り離し**」を参照してください。

（手順 2）待機系 BCU の取り外し

「9.3.1　障害が発生したボードの交換（電源 ON したまま）（1）運用中なので電源 ON したまま，待機系 BCU を交換したい　**（手順 2）待機系 BCU の取り外し**」を参照してください。

〔注意事項〕

感電する恐れがあります。電源を ON したままでのボードの取り外し／取り付け作業は，教育を受けた技術者または保守員にご依頼ください。

（手順 3）運用モードの変更

新しい BCU を待機系に実装するまでの間は障害の検出などを抑止したい場合や，今後一重化で運用したい場合は，装置管理者モードに移行したあと，次に示す set mode コマンドを実行してください。

```
# set mode simplex [Enter]
```

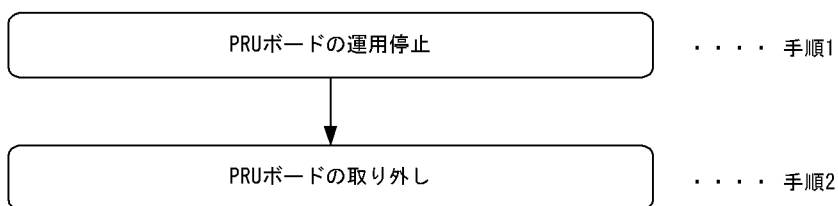
本コマンド実行後，システム操作パネルに二重化関連の障害表示がないことと，show system コマンドを実行して，運用モードが「Simplex」（一重化）となっていることを確認してください。show system コマンドの実行結果を次の図に示します。

図 9-23　show system コマンド実行結果

```
> show system
System : SB-7808R, SB-780S-R Ver. 9.2 [OS-R]
Node : Name=System Name
    Contact=Contact Address
    Locate=Location
    Node Info : Simplex Mode  ◀── 運用モードが「Simplex」（一重化）
     :      :      :      :      :      :
    BCU0 : Active
        RM-CPU : Active SB-BCU-RM8MS[BCU-RM8MS] 0000
        Boot : 2003/01/11 19:27:42 , Power ON , 0 times restart
     :      :      :      :      :      :
    BCU1 : Disconnect  ◀── 待機系は未実装
        RM-CPU : unused
     :      :      :      :      :      :
```

(2) 運用中なので電源 ON したまま，PRU を取り外したい

電源 ON したまま PRU を取り外す概略手順を次の図に示します。

図 9-24　PRU ボード取り外し手順

次に各手順の詳細を記載します。

（手順 1）PRU ボードの運用停止

取り外す PRU の運用を停止します。次に示す close pru コマンドを運用端末から実行します。このとき，対象となる PRU 配下の NIF は運用中であっても停止します。

```
close [-f] pru <PRU No.>[Enter]     ( PRU No.：対象となるPRU番号)
```

システム操作パネルから運用停止させることもできます。この場合，次のとおり操作してください。

<Main Menu>→"Action"⇒<ACTION>→"CLOSE"⇒"PRUx"　(x ： 対象となるPRU番号)を選択

（手順 2）PRU ボードの取り外し

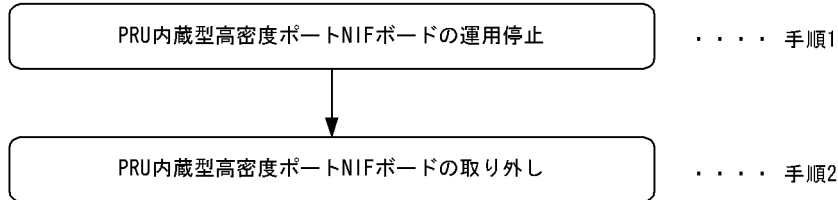
対象となる PRU ボードの STATUS LED 表示が消灯になったことを確認したあと，対象となる PRU ボードに取り付けられている NIF ボードを取り外し，次に PRU ボードを取り外してください。取り外し方法については「ハードウェア取扱説明書」を参照してください。

〔注意事項〕

感電する恐れがあります。電源を ON したままでのボードの取り外し／取り付け作業は，教育を受けた技術者または保守員にご依頼ください。

(3) 運用中なので電源 ON したまま，PRU 内蔵型高密度ポート NIF を取り外したい

電源 ON したまま PRU 内蔵型高密度ポート NIF を取り外す概略手順を次の図に示します。

図 9-25　PRU 内蔵型高密度ポート NIF ボード取り外し手順

次に各手順の詳細を記載します。

(手順 1) PRU 内蔵型高密度ポート NIF ボードの運用停止

取り外す PRU 内蔵型高密度ポート NIF の運用を停止します。次に示す close pru コマンドを運用端末から実行します。このとき，対象となる PRU 内蔵型高密度ポート NIF 配下の NIF は運用中であっても停止します。

```
close [-f] pru <PRU No.>[Enter]    ( PRU No.：対象となるPRU番号)
```

システム操作パネルから運用停止させることもできます。この場合，次のとおり操作してください。

<Main Menu>→”Action”⇒<ACTION>→”CLOSE”⇒”PRUx” (x ： 対象となるPRU番号)を選択

(手順 2) PRU 内蔵型高密度ポート NIF ボードの取り外し

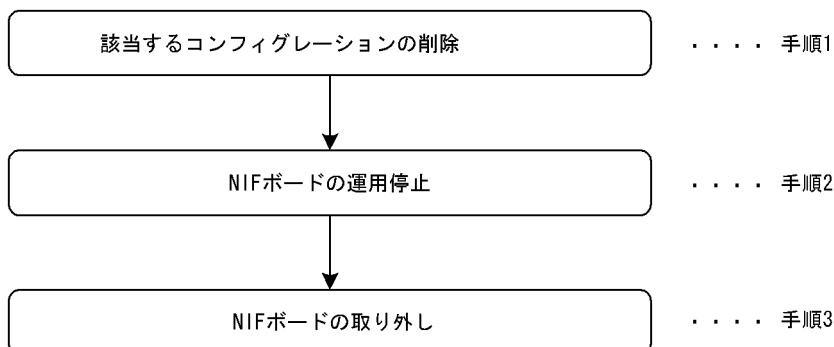
対象となる PRU 内蔵型高密度ポート NIF ボードの STATUS LED 表示が消灯していることを確認したあと，PRU 内蔵型高密度ポート NIF ボードを取り外してください。取り外し方法については「ハードウェア取扱説明書」を参照してください。

〔注意事項〕

感電する恐れがあります。電源を ON したままでのボードの取り外し／取り付け作業は，教育を受けた技術者または保守員にご依頼ください。

(4) 運用中なので電源 ON したまま，NIF を取り外したい

電源 ON したまま NIF を取り外す概略手順を次の図に示します。なお，PRU 内蔵型高密度ポート NIF の場合は以下の手順を実行しても，取り外せません。取り外す方法については，「(3) 運用中なので電源 ON したまま，PRU 内蔵型高密度ポート NIF を取り外したい」を参照してください。

図 9-26　NIF ボード取り外し手順

次に各手順の詳細を記載します。

（手順 1）該当するコンフィグレーションの削除

必要な場合，該当するコンフィグレーションの削除を行います。コンフィグレーションの削除方法については，「コンフィグレーションガイド」を参照してください。

（手順 2）NIF ボードの運用停止

撤去する NIF ボードの運用を停止します。次に示す close nif コマンドを運用端末から実行します。

```
close [-f] nif <NIF No.>[Enter]  ( NIF No.：対象となるNIF番号)
```

システム操作パネルから運用停止させることもできます。この場合，次のとおり操作してください。

<Main Menu>→”Action”⇒<ACTION>→”CLOSE”⇒”NIFxx”　(xx ： 対象となるNIF番号)を選択

（手順 3）NIF ボードの取り外し

対象となる NIF ボードの STATUS LED 表示が消灯していることを確認したあと，NIF ボードを取り外してください。なお，NIF ボードの付属する PRU を運用停止した場合も NIF ボードの STATUS LED 表示が消灯していることを確認したあと，NIF ボードを取り外してください。取り外し方法については「ハードウェア取扱説明書」を参照してください。

〔注意事項〕

感電する恐れがあります。電源を ON したままでのボードの取り外し／取り付け作業は，教育を受けた技術者または保守員にご依頼ください。

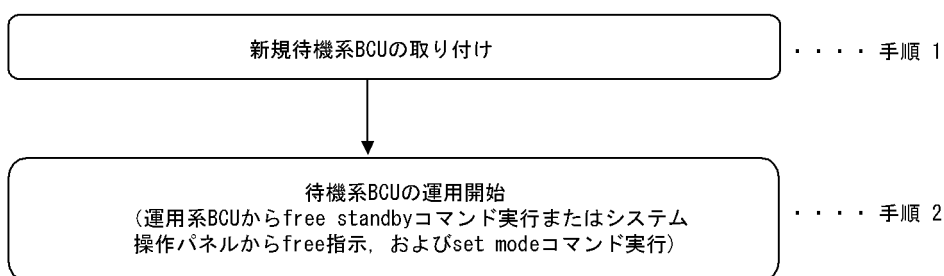
9.4.2　ボードの増設（電源 ON したまま）

ここでは本装置の BCU を 1 枚追加して二重化運用に変更したい場合や，接続回線数増加に伴う PRU または PRU 内蔵型高密度ポート NIF，NIF の増設を行うときの手順を記載しています。増設対象となるボードに応じて，次に記載してある説明を参照してください。なお，各ボードの搭載位置に関する説明および LED に関する説明は「ハードウェア取扱説明書」を参照してください。

(1)　運用中なので電源 ON したまま，待機系用の BCU を増設したい

ここでは，今まで一重化で運用していた装置に BCU を 1 枚追加して二重化運用に変更する手順を記載しています。障害などにより BCU を交換する手順に関しては，「9.4.1　ボードの取り外し（電源 ON したまま）（1）運用中なので電源 ON したまま，待機系 BCU を取り外したい」を参照してください。

電源 ON したまま待機系用の BCU を増設する概略手順を次の図に示します。

図 9-27　待機系 BCU 増設手順

次に各手順の詳細説明を記載します。

（手順 1）新規待機系 BCU の取り付け

「9.3.1 障害が発生したボードの交換（電源 ON したまま）（1）運用中なので電源 ON したまま，待機系 BCU を交換したい （手順 3）待機系 BCU の取り付け」を参照してください。

〔注意事項〕

感電する恐れがあります。電源を ON したままでのボードの取り外し／取り付け作業は，教育を受けた技術者または保守員にご依頼ください。

（手順 2）待機系 BCU の運用開始

一重化で運用していた装置に待機系 BCU を取り付けただけでは，待機系 BCU は運用状態（正常な二重化運用）になりません。（手順 1）終了後，運用系 BCU に接続した運用端末から，次に示す待機系 BCU を運用状態にする free standby コマンドの実行が必要です。

```
> free standby [Enter]
```

システム操作パネルから運用開始させることもできます。この場合，次のとおり操作してください。

```
<Main Menu>→”Action”⇒<ACTION>→”FREE”⇒”standby”を選択
```

次に，運用系 BCU に接続した運用端末から，装置管理者モードに移行したあと，次のコマンドを実行してください。

```
# set mode auto_duplex [Enter] または
# set mode duplex [Enter]
```

本コマンド実行後，装置が正常な二重化運用を実施しているかどうかを確認するため，show system コマンドを実行して，運用モードが「Duplex Mode」（二重化）となっていることを確認してください。

show system コマンドの実行結果を次の図に示します。

図 9-28 show system コマンド実行結果

```
> show system
System : SB-7808R, SB-780S-R Ver. 9.2 [OS-R]
Node : Name=System Name
    Contact=Contact Address
    Locate=Location
```

```
  :     :     :     :     :     :
    BCU0 : Active
        RM-CPU : Active SB-BCU-RM8MS[BCU-RM8MS] 0000
        Boot : 2003/01/11 19:27:42 , Power ON , 0 times restart
  :     :     :     :     :     :
    BCU1 : Standby
        RM-CPU : Active SB-BCU-RM8MS[BCU-RM8MS] 0000
        Boot : 2003/01/11 19:27:43 , Power ON , 0 times restart
  :     :     :     :     :     :
```

待機系は正常運用

〔増設後の注意事項〕

スロット 0，スロット 1 両方の MC スロットに MC を実装している場合，BCU 増設後の初期状態で

はスロット 0 の MC を優先して起動するように設定されています。このため，待機系 BCU のスロット 1 の MC を優先して起動する運用を行いたい場合は，運用系 BCU に接続した運用端末から，装置管理者モードに移行したあと，次に示す set mode コマンドにより，優先 MC スロットの設定を行ってください。

```
# set mode standby slot1 reload [Enter]
```

待機系 BCU 起動時の優先 MC スロットの設定後，運用系 BCU に接続した運用端末から，次に示す reload コマンドにより，待機系 BCU を再起動してください。なお，本コマンドは，装置管理者モードでなくても実行できます。

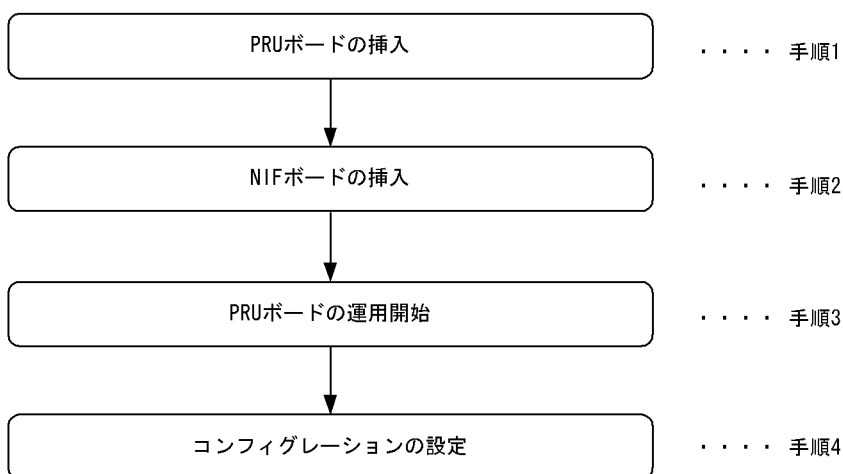
```
> reload dump-image -f standby [Enter]
```

待機系 BCU 再起動後，運用系 BCU に接続した運用端末から，次に示す show system コマンドを実行し，運用モードが「Duplex Mode」（二重化）となっていること，および待機系 BCU の運用状態が「Standby」になっていることを確認してください。show system コマンドの実行結果は，「図 9-28 show system コマンド実行結果」を参照してください。

```
> show system [Enter]
```

（2） 運用中なので電源 ON したまま，PRU ボードを増設したい

電源 ON したまま PRU ボードを増設する概略手順を次の図に示します。

図 9-29　PRU ボード増設手順

次に各手順の詳細説明を記載します。

（手順 1）PRU ボードの挿入

空きスロットに PRU ボードを挿入します。挿入方法については，「ハードウェア取扱説明書」を参照してください。

〔注意事項〕

感電する恐れがあります。電源を ON したままでのボードの取り外し／取り付け作業は，教育を受けた技術者または保守員にご依頼ください。

（手順 2）NIF ボードの挿入

必要であれば，NIF ボードを挿入します。挿入方法については，「ハードウェア取扱説明書」を参照

してください。

挿入する NIF が以下の場合，NIF 挿入前にインタフェースモードを 8k インタフェースモードに設定してください。詳細については「5.4.1　NE1G-48T の実装手順」を参照してください。

- NE1G-48T

〔注意事項〕

感電する恐れがあります。電源を ON したままでのボードの取り外し／取り付け作業は，教育を受けた技術者または保守員にご依頼ください。

（手順 3）PRU ボードの運用開始

増設した PRU ボードの運用を開始します。次に示す free pru コマンドを運用端末から実行します。このとき，配下にある NIF ボードも運用開始されます。

```
free pru <PRU No.>[Enter]     ( PRU No.：対象となるPRU番号)
```

システム操作パネルから運用開始させることもできます。この場合，次のとおり操作してください。

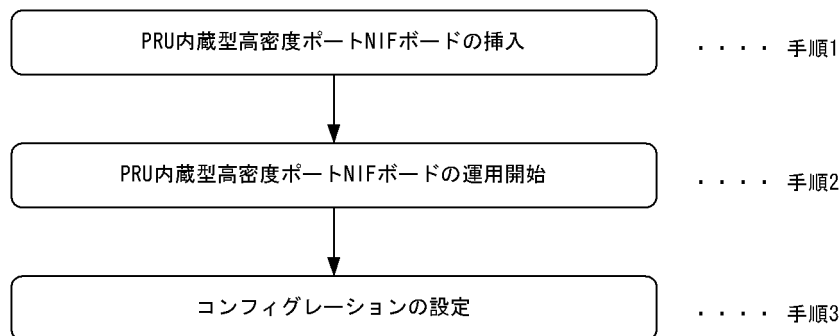
```
<Main Menu>→”Action”⇒<ACTION>→”FREE”⇒”PRUx” (x : 対象となるPRU番号)を選択
```

（手順 4）コンフィグレーションの設定

必要であれば，コンフィグレーションの設定を行います。コンフィグレーションの設定方法については，「コンフィグレーションガイド」を参照してください。

(3) 運用中なので電源 ON したまま，PRU 内蔵型高密度ポート NIF ボードを増設したい

電源 ON したまま PRU 内蔵型高密度ポート NIF ボードを増設する概略手順を次の図に示します。

図 9-30　PRU 内蔵型高密度ポート NIF ボード増設手順

（手順 1）PRU 内蔵型高密度ポート NIF ボードの挿入

空きスロットに PRU 内蔵型高密度ポート NIF ボードを挿入します。挿入方法については，「ハードウェア取扱説明書」を参照してください。

〔注意事項〕

感電する恐れがあります。電源を ON したままでのボードの取り外し／取り付け作業は，教育を受けた技術者または保守員にご依頼ください。

（手順 2）PRU 内蔵型高密度ポート NIF ボードの運用開始

増設した PRU 内蔵型高密度ポート NIF ボードの運用を開始します。次に示す free pru コマンドを運用端末から実行します。このとき，配下にある NIF ボードも運用開始されます。

```
free pru <PRU No.>[Enter]     ( PRU No.：対象となるPRU番号)
```

システム操作パネルから運用開始させることもできます。この場合，次のとおり操作してください。

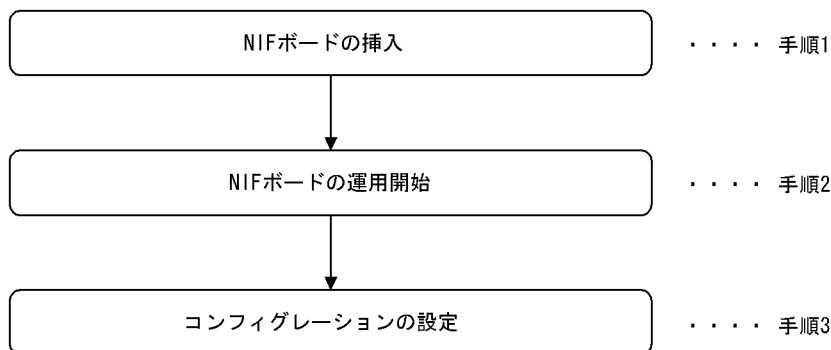
`<Main Menu>→”Action”⇒<ACTION>→”FREE”⇒”PRUx”` (x : 対象となるPRU番号)を選択

（手順 3）コンフィグレーションの設定

必要であれば，回線，物理ポートなどのコンフィグレーションを設定します。コンフィグレーションの設定方法については，「コンフィグレーションガイド」を参照してください。

（4） 運用中なので電源 ON したまま，NIF ボードを増設したい

電源 ON したまま NIF ボードを増設する概略手順を次の図に示します。なお，PRU 内蔵型高密度ポート NIF の場合は以下の手順を実行しても，増設できません。増設方法については，「(3) 運用中なので電源 ON したまま，PRU 内蔵型高密度ポート NIF ボードを増設したい」を参照してください。

図 9-31 NIF ボード増設手順

次に各手順の詳細説明を記載します。

（手順 1）NIF ボードの挿入

挿入する NIF が以下の場合，NIF を挿入する前にインタフェースモードを 8k インタフェースモードに設定してください。詳細については，「5.4.1 NE1G-48T の実装手順」を参照してください。
NIF の空きスロットに NIF ボードを挿入します。挿入方法については，「ハードウェア取扱説明書」を参照してください。

- NE1G-48T

〔注意事項〕

感電する恐れがあります。電源を ON したままでのボードの取り外し／取り付け作業は，教育を受けた技術者または保守員にご依頼ください。

（手順 2）NIF ボードの運用開始

挿入した NIF ボードを運用状態にします。NIF ボードが接続されている PRU ボードが運用状態の場合，次に示す free nif コマンドを運用端末から実行します。

`free nif <NIF No.>[Enter]`　(NIF No.：対象となるNIF番号)

システム操作パネルから運用開始させることもできます。この場合，次のとおり操作してください。

`<Main Menu>→”Action”⇒<ACTION>→”FREE”⇒”NIFxx”` (xx : 対象となるNIF番号)を選択

PRU ボードが停止状態の場合，次に示す free pru コマンドを運用端末から実行します。PRU の運用

開始と共に，NIF ボードは運用開始されます。

free pru <PRU No.>[Enter]　　(PRU No.：対象となるPRU番号)

システム操作パネルから運用開始させることもできます。この場合，次のとおり操作してください。

<Main Menu>→”Action”⇒<ACTION>→”FREE”⇒”PRUx” (x : 対象となるPRU番号)を選択

(手順 3) コンフィグレーションの設定

必要であれば，回線，物理ポートなどのコンフィグレーションを設定します。コンフィグレーションの設定方法については，「コンフィグレーションガイド」を参照してください。

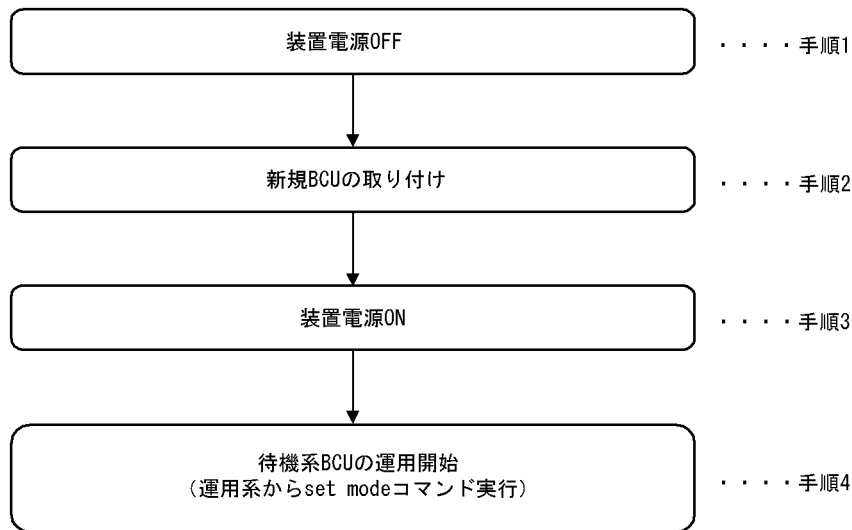
9.4.3 ボードの増設（電源 OFF したあと）

ここでは保守点検などでいったん電源 OFF した場合に，ボードを追加したいときの手順を記載しています。

(1) 保守点検などでいったん電源 OFF したときに，待機系用の BCU を増設したい

ここでは，今まで一重化で運用していた装置の電源をいったん OFF して BCU を 1 枚追加し，二重化運用に変更する手順を記載しています。

いったん電源 OFF して待機系用の BCU を増設する概略手順を次の図に示します。

図 9-32　待機系 BCU 交換手順

次に各手順の詳細説明を記載します。

(手順 1) 装置電源 OFF

装置の電源を落とします。

(手順 2) 新規 BCU の取り付け

「9.3.2　障害が発生したボードの交換（電源 OFF したあと） (1) 電源を OFF して BCU を交換したい　(手順 3) 新規 BCU の取り付け」を参照してください。

(手順 3) 装置電源 ON

装置の電源を ON してください。

〔注意事項〕

電源冗長化時は，すべてのスイッチまたはブレーカをONにしてください。電源ONの方法については，「ハードウェア取扱説明書」を参照してください。

(手順4) 待機系BCUの運用開始

一重化で運用していた装置に待機系BCUを取り付けただけでは，待機系BCUは運用状態（正常な二重化運用）になりません。(手順3) 終了後，運用系BCUに接続された運用端末から，装置管理者モードに移行したあと，次のコマンドを実行してください。

```
# set mode auto_duplex [Enter] または
# set mode duplex [Enter]
```

本コマンド実行後，装置が正常な二重化運用を実施しているかどうかを確認するため，show systemコマンドを実行して，運用モードが「Duplex Mode」（二重化）となっていることを確認してください。show systemコマンドの実行結果を次の図に示します。

図 9-33　show systemコマンド実行結果

```
> show system
System : SB-7808R, SB-780S-R Ver. 9.2 [OS-R]
Node : Name=System Name
    Contact=Contact Address
    Locate=Location
    Node Info : Duplex Mode  ◀──── 運用モードが「Duplex」（二重化）
     :       :       :       :       :       :
    BCU0 : Active
        RM-CPU : Active SB-BCU-RM8MS[BCU-RM8MS] 0000
        Boot : 2003/01/11 19:27:42 , Power ON , 0 times restart
     :       :       :       :       :       :
    BCU1 : Standby  ◀──── 待機系は正常運用
        RM-CPU : Active SB-BCU-RM8MS[BCU-RM8MS] 0000
        Boot : 2003/01/11 19:27:43 , Power ON , 0 times restart
     :       :       :       :       :       :
```

〔増設後の注意事項〕

スロット0，スロット1両方のMCスロットにMCを実装している場合，BCU増設後の初期状態ではスロット0のMCを優先して起動するように設定されています。このため，待機系BCUのスロット1のMCを優先して起動する運用を行いたい場合は，BCU運用系に接続した運用端末から，装置管理者モードに移行したあと，次に示すset modeコマンドにより，優先MCスロットの設定を行ってください。

```
# set mode standby slot1 reload [Enter]
```

待機系BCU起動時の優先MCスロットの設定後，運用系BCUに接続した運用端末から，次に示すreloadコマンドにより，待機系BCUを再起動してください。なお，本コマンドは，装置管理者モードでなくても実行できます。

```
> reload dump-image -f standby [Enter]
```

待機系 BCU 再起動後，運用系 BCU に接続した運用端末から，次に示す show system コマンドを実行し，運用モードが「Duplex Mode」（二重化）となっていること，および待機系 BCU の運用状態が「Standby」になっていることを確認してください。show system コマンドの実行結果は，「図 9-33 show system コマンド実行結果」を参照してください。

```
> show system [Enter]
```

（2） 保守点検などでいったん電源 OFF したときに，PRU を増設したい

「ハードウェア取扱説明書」を参照してください。

（3） 保守点検などでいったん電源 OFF したときに，PRU 内蔵型高密度ポート NIF を増設したい

「ハードウェア取扱説明書」を参照してください。

（4） 保守点検などでいったん電源 OFF したときに，NIF を増設したい

「ハードウェア取扱説明書」を参照してください。

〔増設後の注意事項〕

増設する NIF が以下でコンフィグレーションファイルに 16k インタフェースモードが設定されている場合，装置起動後，インタフェースモードを 8k インタフェースモードに変更してください。詳細については，「5.4.1　NE1G-48T の実装手順」を参照してください。

- NE1G-48T

9.4.4 メモリの増設

本装置は，電源を ON にしたままではメモリを増設できません。必ず電源を OFF にして，メモリの増設を実施してください。

なお，メモリの増設方法については，「ハードウェア取扱説明書」を参照してください。

9.5 MC の取り外し／取り付け

本装置の MC は，予備 MC だけ装置の動作中に抜き差しができます。本装置の動作中に予備 MC の抜き差しを行う場合は次の点に注意してください。

また，誤って本装置の動作中に現用 MC の抜き差しを行ってしまった場合は，電源 OFF ／ ON を実行して本装置を再起動してください。

（1） MC アクセス中の LED が消灯していること

カードスロットごとに MC アクセスを示す LED があります。MC を抜き差しする場合は，LED が消灯している（MC にアクセスしていない）ことを確認してください。LED が点灯しているとき（MC アクセス中）に抜き差しを行うと MC を破損する恐れがあります。

（2） より安全に MC の抜き差しを行うためには

本装置には MC のアクセスを禁止するコマンドがあります。MC アクセス禁止コマンドを実行すると，MC アクセス禁止解除コマンドを実行するまでは，本装置は MC にはアクセスしません（MC アクセス禁止コマンドについては，「運用コマンドレファレンス Vol.1　set mc disable」を参照してください。MC アクセス禁止コマンド実行後は，いったん LED が消灯していることを確認してください。）

（3） MC 抜き差し後に注意すること

コマンド操作を行っているディレクトリが予備 MC 上（例：/secondaryMC/usr/home/operator）の場合，コマンドが実行できなくなることがあります。cd コマンドでホームディレクトリ（例：/primaryMC/usr/home/operator）に移動してからコマンドを再実行してください。

（4） MC 挿入時の注意事項

MC を予備スロットへ挿入したあと，show mc コマンドを使用して，挿入した MC が認識されていることを確認してください。show mc コマンドを実行し，該当する予備 MC のサイズが 0 バイトと表示されている場合は予備 MC が正常にマウントされていません。この場合は，10 秒ほど経過した後に再度確認してください。再度確認しても挿入した MC が認識されていない場合には set mc disable コマンド実行後，MC を抜き，再挿入してください。

9.6　装置／回線の状態を確認する

9.6.1　交換／増設した待機系 BCU の状態確認

ここでは通常運用時や本装置の BCU の交換，増設を行ったあとなどの状態を確認するときの手順を記載しています。また障害のログが出ているときの対応作業の一つとしても参照してください。

まず，運用系に接続した運用端末から，次に示す show system コマンドを実行して，待機系の運用状態を確認してください。

```
> show system [Enter]
```

コマンド実行結果を次の図に示します。待機系 BCU の運用状態を確認してください（次の図では「BCU0」が運用系，「BCU1」が待機系となっています)。

図 9-34　show system コマンド実行結果

```
> show system
System : SB-7808R, SB-780S-R Ver. 9.2 [OS-R]
Node : Name=System Name
    Contact=Contact Address
    Locate=Location
     :       :       :       :       :       :
    BCU0 : Active
        RM-CPU : Active SB-BCU-RM8MS[BCU-RM8MS] 0000
        Boot : 2003/01/11 19:27:42 , Power ON , 0 times restart
     :       :       :       :       :       :
```

```
     :       :       :       :       :       :
```

(a)　待機系の運用状態が「Standby」の場合

正常に運用されています。

(b)　待機系の運用状態が「Fault」の場合

待機系が障害中，または初期化中となっています。待機系 BCU ボードにある STATUS LED が緑点滅状態の場合は初期化中です。待機系が立ち上がると，STATUS LED が緑点灯状態になるので，それまでお待ちください。それ以外の場合は障害中です。show logging コマンドを実行して，待機系 BCU の詳細な情報を収集してください。

(c)　待機系の運用状態が「Closed」の場合

待機系が保守中となっています。この状態では正常な二重化運用ができません。待機系 BCU の交換処理等が終了したら，運用系に接続した運用端末から次に示す free standby コマンドを実行してください。

```
> free standby [Enter]
```

(d) 待機系の運用状態が「Disconnect」の場合

待機系 BCU が未実装です。

(e) 待機系の運用状態が「Configuration Discord」の場合

運用系と待機系のコンフィグレーションが異なっているので，正常な二重化運用ができません。「5.6.2 二重化運用時の注意事項」に従い，両系のコンフィグレーションを一致させてください。

(f) 待機系の運用状態が「Software Version Discord」の場合

運用系と待機系のソフトウェアバージョンが異なっているので，正常な二重化運用ができません。両系のソフトウェアバージョンを一致させてください。

(g) 待機系の運用状態が「License key Discord」の場合

運用系と待機系のソフトウェアライセンスキーが異なっているので，正常な二重化運用ができません。両系のソフトウェアライセンスキーを一致させてください。

9.6.2 交換／増設した PRU ／ NIF の状態確認

ここでは通常運用時や本装置の PRU ／ NIF の交換，増設を行ったあとなどの状態を確認するときの手順を記載しています。また，障害のログが出ているときの対応作業の一つとしても参照してください。

(1) PRU の場合

［実行例］

本装置の PRU 番号 1 の PRU ボードを交換／増設した場合の PRU 状態の確認。

運用端末から次に示す show system コマンドを実行します。

```
> show system[Enter]
```

コマンド実行結果として，「図 9-35　PRU の show system コマンド実行による確認結果」に示す画面を表示するので，次のことを確認してください。

- 該当する PRU が正常に運用（本例では”PRU1: active”）であること
  注　確認時，期待値にならないときは次の確認を行ってください。
- PRU が正常動作しない (”PRU1: active”にならない）場合

1. PRU ボードが挿入されているか。
2. PRU ／ NIF ボードが半挿し状態でないか。
3. 接続している装置の立ち上げが完了しているか。
4. PRU の立ち上げが完了しているか。

図 9-35　PRU の show system コマンド実行による確認結果

```
> show system
:      :      :      :      :      :
    PRU0 : Active SB-PRU-B2 [PRU-B2]
        Lamp : LED=green
        Memory : size=131,072kB(128MB)
    PRU1 : Active SB-PRU-B2 [PRU-B2]
        Lamp : LED=green
        Memory : size=131,072kB(128MB)
    PRU2 : Unused
    PRU3 : Unused
  >
```

（2） NIF(イーサネット) の場合

［実行例］

本装置の NIF 番号 2 に Line 番号 0 のセグメント規格をオートネゴシエーションに設定し，オートネゴシエーションで動作している HUB に接続したあとの回線状態を確認します。運用端末から次に示す show nif コマンドを実行します。

```
> show nif 2[Enter]
```

コマンド実行結果例として，「図 9-36　10BASE-T ／ 100BASE-TX ／ 1000BASE-T NIF の show nif コマンド実行による確認結果」に示す画面を表示します。次のことを確認してください。

- 該当する NIF が正常に運用（本例では”NIF2: active”）であること
- 該当する回線が正常に運用（本例では”Line0: active up”）であること
- Line 種別が接続している装置と合っている（本例では,”100BASE-TX full(auto)”）こと
  確認時，期待値にならないときは次の確認を行ってください。

（a） 10BASE-T/100BASE-TX/1000BASE-T の場合

回線が正常動作しない場合

- ケーブルが抜けていたり半挿し状態でないか。
- 使用しているケーブルはカテゴリ 5 以上で 8 芯 4 対のツイストペアケーブル（UTP）か。
- 全二重固定または半二重固定の設定をしている場合，クロスケーブルまたはストレートケーブルを間違えていないか。
- 接続している装置の立ち上げが完了しているか。

回線タイプが接続している装置と合っていない場合

- 接続している装置の通信速度および通信方式（全二重または半二重）とコンフィグレーションが合っているか。
- 全二重固定の装置と接続するときに本装置のコンフィグレーションをオートネゴシエーションにしていないか。

（b） 1000BASE-X の場合

回線が正常動作しない場合

- ケーブルが抜けていたり半挿し状態でないか。
- 使用しているケーブルのシングルモードまたはマルチモードの種別は正しいか。
- トランシーバが抜けていたり半挿し状態でないか。
- トランシーバが本装置でサポートされているか。
- 相手装置の通信方式を全二重としているか。
- 通信方式を全二重固定の装置と接続するときに本装置のコンフィグレーションをオートネゴシエーションにしていないか。
- 接続している装置の立ち上げが完了しているか。

（c） 10GBASE-R および 10GBASE-W の場合

回線が正常動作しない場合

- ケーブルが抜けていたり半挿し状態でないか。
- 接続している装置の立ち上げが完了しているか。
- トランシーバを交換可能な NIF の場合，以下を確認する。
  - ・トランシーバが抜けていたり半挿し状態でないか。
  - ・トランシーバが本装置でサポートされているか。

図 9-36　10BASE-T ／ 100BASE-TX ／ 1000BASE-T NIF の show nif コマンド実行による確認結果

```
> show nif 2
2003/02/23 12:30:00
NIF2 : active  12-port 10BASE-T/100BASE-TX/1000BASE-T  retry:0
        Average:0/20Gbps  Peak:0Mbps at 00:33:25
 Line0: active up  100BASE-TX(auto),full  00:12:E2:d0:67:68
        Average out:0Mbps  Average in:0Mbps
 Line1: unused  -  00:12:E2:d0:67:69
        Average out:0Mbps  Average in:0Mbps
 Line2: unused  -  00:12:E2:d0:67:6a
        Average out:0Mbps  Average in:0Mbps
 Line3: unused  -  00:12:E2:d0:67:6b
        Average out:0Mbps  Average in:0Mbps
 Line4: unused  -  00:12:E2:d0:67:6c
        Average out:0Mbps  Average in:0Mbps
 Line5: unused  -  00:12:E2:d0:67:6d
        Average out:0Mbps  Average in:0Mbps
 Line6: unused  -  00:12:E2:d0:67:6e
        Average out:0Mbps  Average in:0Mbps
 Line7: unused  -  00:12:E2:d0:67:6f
        Average out:0Mbps  Average in:0Mbps
 Line8: unused  -  00:12:E2:d0:67:70
        Average out:0Mbps  Average in:0Mbps
 Line9: unused  -  00:12:E2:d0:67:71
        Average out:0Mbps  Average in:0Mbps
 Line10: unused -  00:12:E2:d0:67:72
        Average out:0Mbps  Average in:0Mbps
 Line11: unused -  00:12:E2:d0:67:73
        Average out:0Mbps  Average in:0Mbps
```


（3） NIF(POS) の場合

［実行例］

本装置の NIF 番号 2 の Line 番号 0 に OC-192c/STM-64 POS 回線が接続されている場合の回線状態を確認します。運用端末から次に示す show nif コマンドを実行します。

```
> show nif 2[Enter]
```

コマンド実行結果例として，「図 9-37　OC-192c/STM-64 POS NIF の show nif コマンド実行による確認結果」に示す画面を表示します。次のことを確認してください。

- 該当する NIF が正常に運用（本例では”NIF2: active”）であること
- 該当する回線が正常に運用（本例では”Line0: active up”）であること

確認時，期待値にならないときは次の確認を行ってください。

(a) 回線が正常に動作しない場合

- ケーブルが抜けていたり半挿し状態でないか。
- 使用している光ファイバの種別は正しいか。
- トランシーバを交換可能な NIF の場合，以下を確認する。
  - トランシーバが抜けていたり半挿し状態でないか。
  - トランシーバが本装置でサポートされているか。
- 接続している装置の立ち上げが完了しているか。
- 以下の設定が相手装置と一致しているか。
  - クロック
  - CRC 長
  - スクランブル
  - 動作モード
  - セクショントレースメッセージモード

- J0
- RDI モード
- C2

図 9-37　OC-192c/STM-64 POS NIF の show nif コマンド実行による確認結果

```
> show nif 2
2004/02/23 12:30:00
NIF2 : active  1-port OC-192c/STM-64 POS retry:0
         Average:0/20Gbps  Peak:0Mbps at 00:33:25
 Line0: active up  OC-192c/STM-64 POS(G.652-single-mode 40km)
         Average out:0Mbps  Average in:0Mbps
>
```

"active"となっていること

"active up"となっていること

9.7 回線をテストする

9.7.1 イーサネット回線

回線テストでは，指定するテスト種別により，テスト用に送出するフレームまたはデータの折り返し位置が異なります。テスト種別によるフレームの折り返し位置を次の図に示します。

図 9-38 回線テストのテスト種別によるフレームの折り返し位置

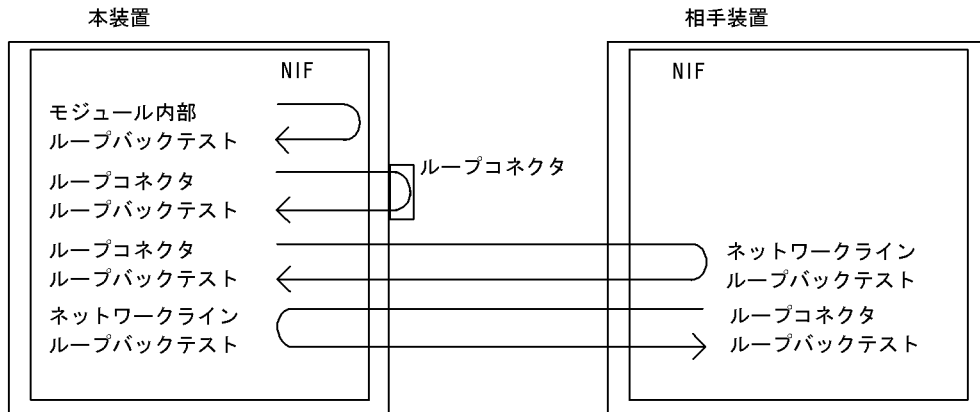



表 9-5 フレーム折り返し位置ごとの回線テスト種別

フレームの折り返し位置	回線テスト種別	確認できる障害部位
NIF	モジュール内部ループバックテスト	NIF（RJ45 コネクタおよびトランシーバを除く）
ループコネクタ	ループコネクタループバックテスト	NIF（RJ45 コネクタおよびトランシーバ含む）
相手装置	ループコネクタループバックテスト	NIF（トランシーバ含む），接続ケーブル，相手装置
本装置のフレーム折り返し設定	ネットワークラインループバックテスト	

また，回線種別により，実行可能なテスト種別が異なります。回線種別と実行可能なテスト種別は，「運用コマンドレファレンス Vol.1 test interfaces（イーサネット）」を参照してください。

次にテスト種別ごとのテスト方法を説明します。

(1) NIF 内でのフレーム折り返しを確認する

NIF 内でのフレーム折り返しを確認する場合，モジュール内部ループバックテストを実行してください。モジュール内部ループバックテストを実行する場合は，close コマンドで回線を閉塞してから行ってください。テストを終了するときは，free コマンドで回線を閉塞状態から運用状態に戻してください。本テストでは，NIF 障害（RJ45 コネクタおよびトランシーバを除く）の有無を確認するため，テスト用フレームを本装置の NIF ボード内で折り返します。本テストは全回線種別で実行できます。本テスト実行中はトランシーバの抜き差しを行わないでください。

テスト例として，NIF 番号 1 の Line 番号 0 で送信間隔 1 秒としてテストを行ったケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
> close nif 1 line 0[Enter]
> test interfaces nif 1 line 0 internal[Enter]
（約1分間待つ）
> no test interfaces nif 1 line 0[Enter]
> free nif 1 line 0[Enter]
```

コマンド実行結果として，「図 9-39　test interfaces，no test interfaces コマンド実行結果例」に示す画面を表示するので，次のことを確認してください。

”Send-NG”および”Receive-NG”が 0 であること。

”Send-NG”および”Receive-NG”が 0 の場合，回線テスト結果は正常です。

”Send-NG”および”Receive-NG”が 0 でない場合は，何らかの異常があるので「運用コマンドレファレンス Vol.1　no test interfaces（イーサネット）」の回線テスト実行結果の表示内容を参照してください。

10GBASE-R および 10GBASE-W で”Send-NG”および”Receive-NG”が 0 でない場合は再度回線テストを実行し，”Send-NG”および”Receive-NG”が 0 であることを確認してください。0 でない場合は何らかの異常があるので「運用コマンドレファレンス Vol.1　no test interfaces（イーサネット）」の回線テスト実行結果の表示内容を参照してください。

図 9-39　test interfaces，no test interfaces コマンド実行結果例

```
> test interfaces nif1 line 0 internal
You have warning message.Use " show warning"  to see them.
> no test interfaces nif1 line 0
You have warning message.Use " show warning"  to see them.
2003/02/23  12:32:00
Interface type             :100BASE-TX
Test count                 :60
Send-OK                    :60          Send-NG                 :0
Receive-OK                 :60          Receive-NG              :0
Data compare error         :0           Out underrun            :0
Out buffer hunt error      :0           Out line error          :0
In CRC error               :0           In frame alignment      :0
In overrun                 :0           In monitor time out     :0
In line error              :0           H/W error               :none
>
```


(2) ループコネクタでのフレーム折り返しを確認する

ループコネクタでのフレーム折り返しを確認する場合，ループコネクタループバックテストを実行してください。ループコネクタループバックテストを実行する場合，およびループコネクタを接続する場合は，close コマンドで回線を閉塞してから行ってください。テストを終了するときは，接続を戻してから free コマンドで回線を閉塞状態から運用状態に戻してください。本テストでは，NIF 障害（RJ45 コネクタおよびトランシーバ含む）を確認するため，テスト用フレームを本装置の NIF ボードに接続したループコネクタ内で折り返します。本テストは全回線種別で実行できます。

回線種別ごとにテストする対象の Line 番号のケーブルを抜いて各回線種別ごとのループコネクタを接続しテストを実施します。ループコネクタ未接続，またはその回線に対応するループコネクタを接続しない場合，正しくテストが実施できないので注意してください。テスト例として，NIF 番号 1 の Line 番号 0 で送信間隔 1 秒としてケーブルを抜いて各回線種別ごとのループコネクタを接続しテストを行ったケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
> close nif 1 line 0[Enter]
（該当ポートにループコネクタを接続する）
> test interfaces nif 1 line 0 connector[Enter]
（約1分間待つ）
> no test interfaces nif 1 line 0[Enter]
（該当ポートのループコネクタを外し，接続を元に戻す）
> free nif 1 line 0[Enter]
```

なお，テスト実行結果の確認は「(1) NIF 内でのフレーム折り返しを確認する」のテスト実行結果と同様に行ってください。

注　1000BASE-LH，10GBASE-ER および 10GBASE-EW でループコネクタループバックテストを行う場合には光アッテネータ（光減衰器）が必要です。光の減衰については次の表を参照してください。

表 9-6　光の減衰

No	回線種別	減衰値（db）
1	1000BASE-LH	5 ～ 20
2	10GBASE-ER	5 ～ 11
3	10GBASE-EW	

(3) 相手装置内でのフレームの折り返しを確認する

相手装置内でのフレーム折り返しを確認する場合，ループコネクタループバックテストを実行してください。ループコネクタループバックテストを実行する場合は，close コマンドで回線を閉塞してから行ってください。テストを終了するときは，free コマンドで回線を閉塞状態から運用状態に戻してください。本テストでは，NIF（トランシーバ含む），接続ケーブル，相手装置の障害を確認するためテスト用フレームを相手装置内で折り返します。本テストは 10GBASE-W だけ実行できます。

相手装置内で折り返す場合のテスト手順を以下に示します。

- 相手装置のテスト対象の回線に対し，テスト用フレームの折り返し設定をする（相手装置でネットワークラインループバックテストを実行する)。
- 本装置でループコネクタループバックテストを実行する。

テスト例として，相手装置の NIF 番号 1 の Line 番号 0 で送信間隔 1 秒で折り返し，本装置の NIF 番号 1 の Line 番号 0 で受信するケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
[本装置]
> close nif 1 line 0[Enter]

[相手装置]
> test interfaces nif 1 line 0 network-line[Enter]
[本装置]
> test interfaces nif 1 line 0 connector[Enter]

（約1分間待つ）
[相手装置][本装置]
```

```
> no test interfaces nif 1 line 0[Enter]

[本装置]
> free nif 1 line 0[Enter]
```

なお，テスト実行結果の確認は「(1) NIF 内でのフレーム折り返しを確認する」のテスト実行結果と同様に行ってください。テストの実行結果は本装置（ループコネクタループバックテストを実行した装置）で確認します。

(4) 相手装置からのフレームの折り返し設定をする

フレームの折り返しを設定する場合，ネットワークラインループバックテストを実行してください。ネットワークラインループバックテストを実行する場合は，相手装置のテスト対象回線を close コマンドで閉塞してから行ってください。テストを終了するときは，相手装置のテスト対象回線を free コマンドで閉塞状態から運用状態に戻してください。本テストは受信したテスト用フレームの折り返し設定だけ行います。10GBASE-W だけ実行できます。相手装置から受信したデータは，物理層フレームごとに折り返します。

本装置の NIF ボード内で折り返す場合のテスト手順を以下に示します。

- 本装置のテスト対象の回線に対し，本装置でネットワークラインループバックテストを実行する。
- 相手装置でループコネクタループバックテストを実行する。

テスト例として，本装置の NIF 番号 1 の Line 番号 0 で折り返し，相手装置の NIF 番号 1 の Line 番号 0 で送信間隔 1 秒で受信するケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
[相手装置]
> close nif 1 line 0[Enter]

[本装置]
> test interfaces nif 1 line 0 network-line[Enter]
[相手装置]
> test interfaces nif 1 line 0 connector[Enter]

（約1分間待つ）
[本装置][相手装置]
> no test interfaces nif 1 line 0[Enter]

[相手装置]
> free nif 1 line 0[Enter]
```

注　本テストは，受信データの折り返し設定だけを行うため，テスト結果表示はありません。テスト結果は相手装置で確認できます。このため，テスト間隔，テストパターン番号，テストデータ長は，指定不可となります。

9.7.2 POS 回線

回線テストでは，指定するテスト種別により，テスト用に送出するフレームまたはデータの折り返し位置が異なります。テスト種別によるフレームの折り返し位置を次の図に示します。

図 9-40　回線テストのテスト種別によるフレームの折り返し位置

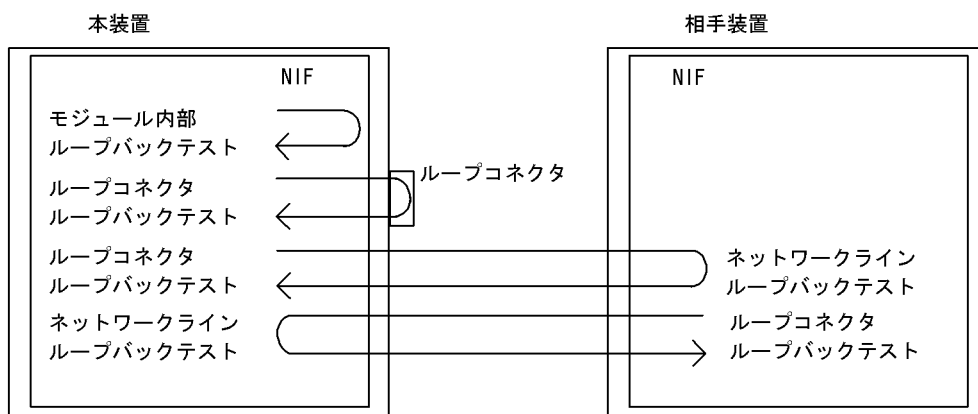



表 9-7　フレーム折り返し位置ごとの回線テスト種別

フレームの 折り返し位置	回線テスト種別	確認できる障害部位
NIF	モジュール内部ループバックテスト	NIF（トランシーバを除く）
ループコネクタ	ループコネクタループバックテスト	NIF（トランシーバ含む）
相手装置	ループコネクタループバックテスト	NIF（トランシーバ含む），接続ケーブル，相手装置
本装置のフレーム折り返し設定	ネットワークラインループバックテスト	

また，コマンドの詳細は，「運用コマンドレファレンス Vol.1　test interfaces（POS）」を参照してください。

次にテスト種別ごとのテスト方法を説明します。

（1） NIF 内でのフレーム折り返しを確認する

NIF 内でのフレーム折り返しを確認する場合，モジュール内部ループバックテストを実行してください。モジュール内部ループバックテストを実行する場合は，close コマンドで回線を閉塞してから行ってください。テストを終了するときは，free コマンドで回線を閉塞状態から運用状態に戻してください。本テストでは，NIF 障害（トランシーバを除く）の有無を確認するため，テスト用フレームを本装置の NIF ボード内で折り返します。本テストは全回線種別で実行できます。本テスト実行中はトランシーバの抜き差しを行わないでください。

テスト例として，NIF 番号 1 の Line 番号 0 で送信間隔 1 秒としてテストを行ったケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
> close nif 1 line 0[Enter]
> test interfaces nif 1 line 0 internal[Enter]
（約1分間待つ）
> no test interfaces nif 1 line 0[Enter]
> free nif 1 line 0[Enter]
```

コマンド実行結果として，「図 9-41　test interfaces，no test interfaces コマンド実行結果例」に示す画面を表示するので，次のことを確認してください。

”Send-NG”および”Receive-NG”が 0 であること。

”Send-NG”および”Receive-NG”が 0 の場合，回線テスト結果は正常です。

”Send-NG”および”Receive-NG”が 0 でない場合は，何らかの異常があるので「運用コマンドレファレンス Vol.1　no test interfaces（POS)」の回線テスト実行結果の表示内容を参照してください。

図 9-41　test interfaces，no test interfaces コマンド実行結果例

```
> test interfaces nif 1 line 0 internal
You have warning message.Use " show warning"  to see them.
> no test interfaces nif 1 line 0
You have warning message.Use " show warning"  to see them.
2004/02/23 12:32:00
Interface type              :OC-192c/STM-16 POS(G.652-single-mode 40km)
Test count                  :60
Send-OK                     :60          Send-NG                 :0
Receive-OK                  :60          Receive-NG              :0
Data compare error          :0           Out underrun            :0
Out buffer hunt error       :0           In CRC error            :0
In short frame              :0           In abort frame          :0
In monitor time out         :0           H/W error               :none
>
```


(2) ループコネクタでのフレーム折り返しを確認する

ループコネクタでのフレーム折り返しを確認する場合，ループコネクタループバックテストを実行してください。ループコネクタループバックテストを実行する場合，およびループコネクタを接続する場合は，close コマンドで回線を閉塞してから行ってください。テストを終了するときは，接続を戻してから free コマンドで回線を閉塞状態から運用状態に戻してください。本テストでは，NIF 障害（トランシーバ含む）を確認するため，テスト用フレームを本装置の NIF ボードに接続したループコネクタ内で折り返します。本テストは全回線種別で実行できます。

回線種別ごとにテストする対象の Line 番号のケーブルを抜いて各回線種別ごとのループコネクタを接続しテストを実施します。ループコネクタ未接続，またはその回線に対応するループコネクタを接続しない場合，正しくテストが実施できないので注意してください。テスト例として，NIF 番号 1 の Line 番号 0 で送信間隔 1 秒としてケーブルを抜いて各回線種別ごとのループコネクタを接続しテストを行ったケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
> close nif 1 line 0[Enter]
```

（該当ポートにループコネクタを接続する）

```
> test interfaces nif 1 line 0 connector[Enter]
```

（約1分間待つ）

```
> no test interfaces nif 1 line 0[Enter]
```

（該当ポートのループコネクタを外し，接続を元に戻す）

```
> free nif 1 line 0[Enter]
```

なお，テスト実行結果の確認は「(1) NIF 内でのフレーム折り返しを確認する」のテスト実行結果と同様に行ってください。

注　OC-48c ／ STM-16 POS(40km) および OC-192c ／ STM-64 POS(40km) でループコネクタループバックテストを行う場合には光アッテネータ（光減衰器）が必要です。光の減衰については次の表を参照してください。

表 9-8　光の減衰

No	回線種別	減衰値（db）
1	OC-48c ／ STM-16 POS(40km)	15 ～ 18
2	OC-192c ／ STM-64 POS(40km)	5 ～ 11

(3) 相手装置内でのフレームの折り返しを確認する

相手装置内でのフレーム折り返しを確認する場合，ループコネクタループバックテストを実行してください。ループコネクタループバックテストを実行する場合は，close コマンドで回線を閉塞してから行ってください。テストを終了するときは，free コマンドで回線を閉塞状態から運用状態に戻してください。本テストでは，NIF（トランシーバ含む），接続ケーブル，相手装置の障害を確認するためテスト用フレームを相手装置内で折り返します。

相手装置内で折り返す場合のテスト手順を以下に示します。

- 相手装置のテスト対象の回線に対し，テスト用フレームの折り返し設定をする（相手装置でネットワークラインループバックテストを実行する)。
- 本装置でループコネクタループバックテストを実行する。

テスト例として，相手装置の NIF 番号 1 の Line 番号 0 で折り返し，本装置の NIF 番号 1 の Line 番号 0 で送信間隔 1 秒で受信するケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
[本装置]
> close nif 1 line 0[Enter]

[相手装置]
> test interfaces nif 1 line 0 network-line[Enter]
[本装置]
> test interfaces nif 1 line 0 connector[Enter]

（約1分間待つ）
[相手装置][本装置]
> no test interfaces nif 1 line 0[Enter]

[本装置]
> free nif 1 line 0[Enter]
```

なお，テスト実行結果の確認は「(1) NIF 内でのフレーム折り返しを確認する」のテスト実行結果と同様に行ってください。テストの実行結果は本装置（ループコネクタループバックテストを実行した装置）で確認します。

(4) 相手装置からのフレームの折り返し設定をする

フレームの折り返しを設定する場合，ネットワークラインループバックテストを実行してください。ネットワークラインループバックテストを実行する場合は，相手装置のテスト対象回線を close コマンドで閉塞してから行ってください。テストを終了するときは，相手装置のテスト対象回線を free コマンドで閉塞

状態から運用状態に戻してください。本テストは受信したテスト用フレームの折り返し設定だけ行います。相手装置から受信したデータは，物理層フレームごとに折り返します。本テストは全回線種別で実行できます。

本装置の NIF ボード内で折り返す場合のテスト手順を以下に示します。

- 本装置のテスト対象の回線に対し，本装置でネットワークラインループバックテストを実行する。
- 相手装置でループコネクタループバックテストを実行する。

テスト例として，本装置の NIF 番号 1 の Line 番号 0 で折り返し，相手装置の NIF 番号 1 の Line 番号 0 で送信間隔 1 秒で受信するケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

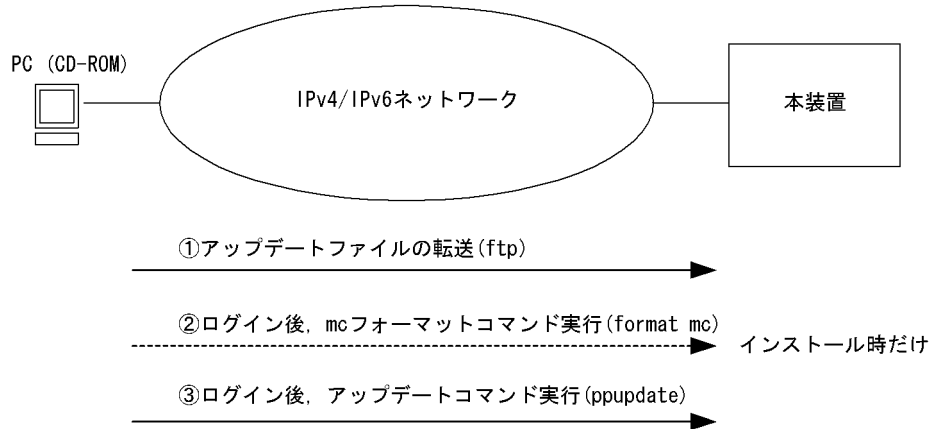
```
[相手装置]
> close nif 1 line 0[Enter]

[本装置]
> test interfaces nif 1 line 0 network-line[Enter]
[相手装置]
> test interfaces nif 1 line 0 connector[Enter]

（約1分間待つ）
[本装置][相手装置]
> no test interfaces nif 1 line 0[Enter]

[相手装置]
> free nif 1 line 0[Enter]
```

注　本テストは，受信データの折り返し設定だけを行うため，テスト結果表示はありません。テスト結果は相手装置で確認できます。このため，テスト間隔，テストパターン番号，テストデータ長は，指定不可となります。

10 ソフトウェアアップデート

この章では，ソフトウェアのアップデートやインストールの概念，代表的なトラブルについて説明します。実際のアップデート，インストール手順については，ソフトウェア添付資料「インストールガイド」を参照してください。

10.1 概要

ソフトウェアのアップデートは，PC などのリモート運用端末からアップデートファイルを装置に転送し，アップデートコマンド（ppupdate）を実行することによって行います。なお，インストール時にはフォーマットコマンド（format mc）の実行が別途必要となります。

アップデートとは

アップデートとは，旧バージョンのソフトウェアから新バージョンのソフトウェアにバージョンアップを行うことをいいます。

アップデートは，アップデート用のファイルを本装置に転送し，ppupdate コマンドを実行することにより行います。アップデートの場合，装置コンフィグレーションおよびユーザ情報（ログインアカウント，パスワードなど）はそのまま引き継がれます。

インストールとは

インストールとは，予備 MC スロット（secondary）の MC に対して新規にソフトウェアをインストールすることをいいます。

インストールは，アップデート用のファイルを本装置に転送し，予備 MC スロットの MC を format mc コマンドでフォーマットして ppupdate コマンドを予備 MC に対して実行することにより行います。インストールの場合，装置コンフィグレーションおよびユーザ情報は初期状態（工場出荷時の状態）となります。インストールは予備 MC に対してだけ実行できます。

アップデートおよびインストールはどちらの場合も，CD-ROM 内のアップデート用ファイルを装置に転送後，ppupdate コマンドを実行することにより行います。

10.2　アップデート後の作業

本装置のソフトウェアアップデート時に発生する代表的なトラブルについて，対処方法を次に示します。その他のトラブルと対処方法については，ソフトウェア添付資料「インストールガイド」を参照してください。

（1） 装置が立ち上がらない

1. ソフトウェアアップデートが正常に終了しなかった可能性があります。ソフトウェアを再インストールしてください。
2. アップデート前のコンフィグレーションをバックアップしてある場合，コンフィグレーションをバックアップからコピーしてください。アップデート前のコンフィグレーションをバックアップしていない場合は，装置を起動後，再作成してください。
3. 装置を再立ち上げしてください。

（2） 装置は立ち上がるが正常に動作しない

1. コンフィグレーションが機器構成と合っていない可能性があります。ソフトウェアアップデートと合わせてコンフィグレーションの変更や機器の増移設を行った場合は，変更内容および増移設した機器を再確認してください。

新ソフトウェアでは，旧ソフトウェアとコンフィグレーションパラメータのデフォルト値が異なっていることがあります。ソフトウェア添付資料を参照のうえ，コンフィグレーション・機器構成を再確認してください。

付録

付録 A　用語解説

（英字）

ARP（Address Resolution Protocol）
IPv4 ネットワークで使用する通信プロトコルです。

AS（Autonomous System）
単一の管理権限で運用している独立したネットワークシステムのことを指します。

AS 境界ルータ
OSPF を使用して，AS 外経路を OSPF 内に導入するルータです。

BGP4（Border Gateway Protocol - version 4）
IPv4 ネットワークで使用する経路制御プロトコルです。

BGP4+（Multiprotocol Extensions for Border Gateway Protocol - version 4）
IPv6 ネットワークで使用する経路制御プロトコルです。

BGP4+ スピーカ
BGP4+ が動作するルータのことです。

BGP スピーカ
BGP が動作するルータのことです。

BPDU（Bridge Protocol Data Unit）
ブリッジ間でやり取りされるフレームです。

CP 輻輳制御
BCU 内の CP で行う輻輳制御方式のことです。
自装置宛のフレームの輻輳を検知すると，その要因のフレームの受信を止めます。この制御の繰り返しによって，正常に動作している VLAN を収容しているポートの自宛通信への影響を抑えられます。

DHCP（Dynamic Host Configuration Protocol）
ネットワーク接続時に IP アドレスを自動設定するプロトコルです。リレーエージェント機能，サーバ機能およびクライアント機能があります。

DHCP/BOOTP リレーエージェント機能
DHCP/BOOTP サーバと DHCP/BOOTP クライアントが異なるサブネットにあるとき，コンフィグレーションで設定したサーバの IP アドレスを DHCP/BOOTP パケットの宛先 IP アドレスに設定して，パケットをサブネット間中継する機能です。

DHCP サーバ機能
IPv4 DHCP クライアントに対して，IP アドレスなどの環境情報（構成情報）を動的に割り当てるための機能です。

Diff-serv（Differentiated services）機能
IP パケットのヘッダ情報から優先度を決定して，その優先度に従ってルータが処理する機能です。

DNS リレー
DNS(Domain Name System) システムの異なるサブネットワークに存在するサーバとクライアント間で，クライアントからのパケットをドメインネームサーバのアドレスに中継する機能です。

DSCP（Differentiated Services Code Point）
IP フローの IP ヘッダ内 DS Field の上位 6 ビットです。

DS ドメイン
Diff-serv 機能を提供するネットワークです。

DVMRP（Distance Vector Multicast Routing Protocol）
IPv4 マルチキャストで使用する距離ベクトル型の経路制御プロトコルです。

EFM（Ethernet in the First Mile）
IEEE802.3ah 規格のことです。

FDB（Filtering Data Base）
トランスペアレント・ブリッジで使用されるテーブルです。FDB にはフレームの送信元 MAC アドレス，フレームを受信したポートおよび監視時刻が記録されます。

ICMP（Internet Control Message Protocol）
IPv4 ネットワークで使用する通信プロトコルです。

ICMPv6（Internet Control Message Protocol version 6）
IPv6 ネットワークで使用する通信プロトコルです。

IGMP（Internet Group Management Protocol）
IPv4 ネットワークで使用するホスト - ルータ間のマルチキャストグループ管理プロトコルです。

IPv4（Internet Protocol version 4）
32 ビットの IP アドレスを持つインターネットプロトコルです。

IPv4 マルチキャスト
IPv4 マルチキャストは，ネットワーク内で選択されたグループに対して同一の情報を送信します。マルチキャストは送信者が受信者ごとにデータを複製する必要がないため，受信者の数に関係なくネットワークの負荷が軽減します。

IPv6（Internet Protocol version 6）
128 ビットの IP アドレスを持つインターネットプロトコルです。

IPv6 DHCP サーバ機能
IPv6 DHCP クライアントに対して，プレフィックス，DNS サーバアドレスなどの環境情報 (構成情報) を動的に割り当てるための機能です。

IPv6 グローバルアドレス
アドレスプレフィックスの上位 3 ビットが 001 で始まるアドレスです。経路情報の集約を目的とした階層形式になっています。IPv6 グローバルアドレスは世界で一意なアドレスで，インターネットを使用した通信に使用されます。

IPv6 サイトローカルアドレス
アドレスプレフィックスの上位 10 ビットが 1111 1110 11 で，64 ビットのインタフェース ID 部を含むアドレスです。同一サイト内だけで有効なアドレスで，インターネットに接続されていないネットワークで自由に IPv6 アドレスを付ける場合に使用されます。

IPv6 マルチキャスト
IPv6 マルチキャストは IPv4 マルチキャストと同様の機能を IPv6 で実現します。

IPv6 リンクローカルアドレス
アドレスプレフィックスの上位 64 ビットが fe80:: で，64 ビットのインタフェース ID 部を含むアドレスです。同一リ

ンク内だけで有効なアドレスで，自動アドレス設定，近隣探索，またはルータがないときに使用されます。

IS-IS

IS-IS は，ルータ間の接続の状態から構成されるトポロジに基づき最短経路を計算するリンクステートプロトコルです。

LLDP（Link Layer Discovery Protocol）

隣接する装置情報を収集するプロトコルです。

MIB（Management Information Base）

機器についての情報を表現するオブジェクトです。SNMP プロトコルで使用します。

MLD（Multicast Listener Discovery）

ルータ - ホスト間で使用される IPv6 マルチキャストグループ管理プロトコルです。

NAT（Network Address Translation）

ローカルネットワークのプライベートアドレスをインターネットなどで使用するグローバルアドレスに変換する機能です。

NDP（Neighbor Discovery Protocol）

IPv6 ネットワークで使用する通信プロトコルです。

NetFlow 統計

ネットワークを流れるトラフィックをサンプリングしてモニタし，モニタした NetFlow 統計情報を NetFlow コレクタと呼ばれる装置に集めて分析することによって，ネットワークの利用状況を把握する機能です。

NIF（Network Interface board）

接続する各メディアに対応したインタフェースを持つコンポーネントです。物理レイヤを処理します。

OADP（Octpower Auto Discovery Protocol）

OADP PDU（Protocol Data Unit）のやりとりによって隣接装置の情報を収集し，隣接装置の接続状況を表示する機能です。

OAM（Operations, Administration, and Maintenance）

ネットワークでの保守運用管理のことです。

OSPF（Open Shortest Path First）

IPv4 ネットワークで使用する経路制御プロトコルです。

OSPFv3

IPv6 ネットワークで使用する経路制御プロトコルです。

OSPF ドメイン

本装置と接続している独立した各 OSPF ネットワークのことです。

OSPF マルチバックボーン

本装置で 1 台のルータ上で複数の OSPF ネットワークと接続して，OSPF ネットワークごとに個別に経路の交換，生成などを行う機能です。

PHB（Per Hop Behavior）

インテリアリードで DSCP に基づいた優先転送動作のことをいいます。

PIM-DM（Protocol Independent Multicast-Dense Mode）

DVMRP のように基盤になっているユニキャスト IPv4 の経路モジュールに依存しないでマルチキャストの経路制御ができるプロトコルです。パケットの送信後，不要な経路を除外します。

PIM-SM（Protocol Independent Multicast-Sparse Mode）
DVMRP のように基盤になっているユニキャスト IPv4 の経路モジュールに依存しないでマルチキャストの経路制御ができるプロトコルです。ランデブーポイントへのパケット送信後，Shortest path で通信します。

PIM-SSM （Protocol Independent Multicast-Source Specific Multicast）
PIM-SM の拡張機能で，ランデブーポイントを使用しないで最短パスで通信する経路制御プロトコルです。

PPP（Point-to-Point Protocol）
シリアル回線用の通信プロトコルです。非同期接続ができます。

PRU（Packet Routing Module）
パケットルーティングモジュールです。パケット転送エンジンとルーティング・QoS テーブル検索エンジンを持ち，ルーティングテーブル，フィルタリング・テーブル，QoS テーブルを検索して，IP パケットを送受信します。

QoS（Quality of Service）制御
実時間型・帯域保証型トラフィックに対して，通信の遅延やスループットなどの通信品質を制御する機能です。

RADIUS（Remote Authentication Dial In User Service）
NAS(Network Access Server) に対して認証・課金を提供するプロトコルです。

RFC（Request For Comments）
TCP/IP に関する仕様を記述している公開文書です。

RIP（Routing Information Protocol）
IPv4 ネットワークで使用する経路制御プロトコルです。

RIPng（Routing Information Protocol next generation）
IPv6 ネットワークで使用する経路制御プロトコルです。

RM（Routing Manager）
ルーティングマネージャです。装置全体の管理およびルーティングプロトコル処理を行います。また，ルーティングテーブルを作成・更新して PRU に配布します。

RMON（Remote Network Monitoring）
イーサネット統計情報を提供する機能です。

RTT（Round Trip Time）
ラウンド・トリップ・タイム。パケットがネットワークを一往復する時間です。

sFlow 統計
sFlow 統計はエンド - エンドのトラフィック（フロー）特性や隣接するネットワーク単位のトラフィック特性の分析を行うため，ネットワークを流れるトラフィックを中継装置（ルータやスイッチ）でモニタする機能です。

SNMP（Simple Network Management Protocol）
ネットワーク管理プロトコルです。

TACACS+（Terminal Access Controller Access Control System Plus）
NAS(Network Access Server) に対して認証・課金を提供するプロトコルです。

Tag-VLAN
IEEE が標準化した VLAN の一つで，イーサネットフレームに Tag と呼ばれる識別子を埋め込むことで VLAN 情報を離れたセグメントに伝えることができる VLAN です。

UDLD（Uni-Directional Link Detection）
片方向リンク障害を検出する機能です。

UDP（User Datagram Protocol）
トランスポート層の通信プロトコルです。

UPC（Usage Parameter Control）
最大帯域制限，最低帯域監視を行う機能です。

VRRP（Virtual Router Redundancy Protocol）
ルータに障害が発生した場合でも，同一イーサネット上の別ルータを経由して通信経路を確保する，ホットスタンバイ機能です。この機能を使用すると，同一イーサネット上の複数ルータから構成される仮想ルータを定義できます。エンドホスト側はデフォルトとして仮想ルータを設定しておけば，ルータに障害が発生した場合でも別ルータの切り替えを意識する必要がありません。

（ア行）

イコールコストマルチパス
ある 2 点間にコストが同じ経路が複数ある場合に，この複数の経路のことをイコールコストマルチパスといいます。

インターナルピア
同じ AS 内に属し，物理的に直接接続された BGP スピーカ間に形成するピアです。ピアリングに使用する IP アドレスは直接接続されたインタフェースのインタフェースアドレスを使用します。

インタフェース
本装置で IP アドレスを付与する単位です。

インデックス
MIB を限定するための情報です。

インテリアノード
DS ドメインで，DSCP に基づいた転送動作だけを行うノードです。

インポート・フィルタ
指定プロトコルで受信したルーティング・パケットの経路情報をルーティングテーブルに取り込むかどうかをフィルタリング条件に従って制御します。

運用端末
本装置の運用管理に使用するコンソールまたはリモート運用端末のことを運用端末と呼びます。

エキスターナルピア
異なる AS に属する BGP スピーカ間に形成するピアです。ピアリングに使用する IP アドレスは直接接続されたインタフェースのインタフェースアドレスを使用します。

エキスポート・フィルタ
ルータ上で同時に動作しているルーティングプロトコル間での経路情報の再配布を制御します。エキスポート・フィルタでは配布先プロトコルのフィルタリング条件と学習元プロトコルのフィルタリング条件によって，特定の宛先に特定の経路情報を送出します。

エリアボーダルータ
複数のエリアに所属するルータです。所属するすべてのエリアについて，個別に経路選択を行います。

オブジェクト ID
MIB を特定するための識別 ID です。root から各ノードの数値をならべて番号をつけることで，MIB を一意に識別でき

ます。

（カ行）

仮想リンク
仮想の回線のことです。仮想リンクの実際の経路があるエリアのことを仮想リンクの通過エリアといいます。

均等最低帯域保証
送信帯域の均等最低保証を行う機能です。キューごとに割り当てられた帯域分だけを送信します。ただし，回線の帯域が空いていれば，空いている帯域も使用して送信します。

均等保証
出力キューからパケットを送信するときの送信順を，1 キュー当たり 1 パケットにして各キューから順番に送信する機能です。

クラシファイア
TCP/IP ヘッダからフローを識別して，個々のユーザとの契約に基づいて DSCP に分類・集約する機能です。バウンダリノードが持っている機能です。

コンフィグレーションファイル
ネットワークの運用環境に合わせて構成および動作条件を設定するファイルです。このファイルはテキストファイル形式で MC に格納します。コンフィグレーションファイルには次に示す種類があります。

- スタートアップコンフィグレーションファイル
  本装置の立ち上げに使用します。このコンフィグレーションに従って運用されます。
- バックアップコンフィグレーションファイル
  スタートアップコンフィグレーションファイルのコピー，または将来のネットワークの変更に備えた編集用として使用します。
- 一時保存コンフィグレーションファイル
  運用中にコンフィグレーションを変更して MC に格納した場合に，編集前のスタートアップコンフィグレーションファイルを一時保存したものです。

（サ行）

最低帯域保証
送信帯域の最低保証を行う機能です。キューごとに指定された帯域分だけを送信します。ただし，回線の帯域が空いていれば，空いている帯域も使用して送信します。

シェーパ
バウンダリノードで送信帯域を制御する機能です。

重要パケット保護機能
保証帯域内で，重要なパケットは優先的に保証帯域内パケットとして転送し，通常のパケットは重要なパケットが全保証帯域を使用して転送していない場合に保証帯域内パケットとして転送する機能です。

出力優先制御
出力優先度に従って優先パケットの追い越しを行う制御です。出力優先度の高いキューに積まれたパケットをすべて送信したあとで，より低いキューに積まれたパケットを送信します。

スタティックルーティング
ユーザがコンフィグレーションによって経路情報を設定するルーティング方法です。

ステートレスアドレス自動設定機能
IPv6 リンクローカルアドレスを装置内で自動生成する機能，ホストが IPv6 アドレスを自動生成するときに必要な情報

を通知する機能です。

スパニングツリー・アルゴリズム

ブリッジによるルーティングで使用されるアルゴリズムで，論理的木構造を形成します。このアルゴリズムによって任意の二つの ES 間で単一の経路を決定でき，フレームのループ周回を防ぐことができます。

スループット

コンピュータ間の通信での実質的な通信速度（実行速度）のことです。

（タ行）

帯域制御

物理ポート単位の最大帯域制限，およびキューごとの最低帯域監視，最大帯域制限，余剰帯域分配を行う機能です。

ダイナミックルーティング

ルーティングプロトコルによってネットワーク内の他ルータと経路情報を交換して経路を選択するルーティング方法です。

トラップ

SNMP エージェントから SNMP マネージャに非同期に通知されるイベント通知です。

（ハ行）

ハードウェアキュー長

1 回の送信処理で回線ハードウェアに与える送信データ長。

バウンダリノード

DS ドメインで，フローを識別して DSCP へ集約して DSCP に基づいて転送動作を行うノードです。

標準 MIB

RFC で規定された MIB です。

フィルタリング

受信したある特定の IP パケットを中継または廃棄する機能です。

プライベート MIB

装置の開発ベンダーが独自に提供する MIB です。

ポリシー

どの業務データを優先的に配信するかという方針を指します。

ポリシーインタフェース情報

ポリシールーティングに従ってパケットを転送するときの，コンフィグレーションで定義したインタフェース情報です。単一または複数のポリシーインタフェース情報をグループ化してポリシーグループ情報を定義します。

ポリシールーティング

ルーティングプロトコルで登録された経路情報に従わないで，ユーザが設定したポリシーをベースにして特定のインタフェースにパケットを転送するルーティング方法です。

（マ行）

マーカー
IP ヘッダの DS フィールドに DSCP 値を書き込む機能です。バウンダリノードが持っている機能です。

マルチキャスト
ネットワーク内で選択されたグループに属している通信先に対して同一の情報を送信する機能です。

マルチキャストグループマネージメント機能
ホスト・ルータ間でのグループメンバーシップ情報の送受信によって，ルータが直接接続したネットワーク上のマルチキャストグループメンバーの存在を学習する機能です。

マルチキャストトンネル機能
二つのマルチキャストルータがユニキャストルータを経由して接続されている場合に，マルチキャストパケットをカプセル化してデータを送受信して，二つのマルチキャストネットワークを接続する機能です。

マルチパス
宛先のネットワークアドレスに対して複数の経路を構築する接続方式です。

未指定アドレス
すべてのビットが 0 のアドレス 0:0:0:0:0:0:0:0(0::0，または ::) は未指定アドレスと定義されます。未指定アドレスはインタフェースにアドレスがないことを表します。

（ヤ行）

優先 MC スロット指定機能
装置を起動するための優先 MC スロットを指定する機能です。

（ラ行）

ルーティングピア
同じ AS 内に属し，物理的に直接接続されない BGP スピーカ間に形成するピアです。ピアリングに使用する IP アドレスはそのルータの装置アドレス，またはルータ内のインタフェースのインタフェースアドレスのどちらかです。

ルート・フラップ・ダンピング
経路情報が頻発してフラップするような場合に，一時的に該当する経路の使用を抑制して，ネットワークの不安定さを最小限にする機能です。

ルート・リフレクション
AS 内でピアを形成する内部ピアの数を減らすための方法です。内部ピアで配布された経路情報をそのほかの内部ピアに再配布して，AS 内の内部ピアの数を減らします。

ルート・リフレッシュ
変化が発生した経路だけを広告する BGP4+ で，すでに広告された経路を強制的に再広告させる機能です。

ループバックアドレス
アドレス 0:0:0:0:0:0:0:1(0::1，または ::1) はループバックアドレスと定義されています。ループバックアドレスは自ノード宛てに通信するときに，パケットの宛先アドレスとして使用されます。ループバックアドレスをインタフェースに割り当てることはできません。

ロードバランス機能
マルチパスを使用して既存回線を集合して高帯域を供給するための機能です。